IBM

International Technical Support Centers

Inside OS/2 Warp Server, Volume 1: Exploring the Core Components

SG24-4602-00

SG24-4602-00

Inside OS/2 Warp Server, Volume 1: Exploring the Core Components

March 1996

Take Note!

Before using this information and the product it supports, be sure to read the general information under "Special Notices" on page xix.

First Edition (March 1996)

This edition applies to IBM OS/2 Warp Server Version 4.

Order publications through your IBM representative or the IBM branch office serving your locality. Publications are not stocked at the address given below.

An ITSO Technical Bulletin Evaluation Form for reader's feedback appears facing Chapter 1. If the form has been removed, comments may be addressed to:

IBM Corporation, International Technical Support Organization
Dept. JN9B Building 045 Internal Zip 2834
11400 Burnet Road
Austin, Texas 78758-3493

When you send information to IBM, you grant IBM a non-exclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

© Copyright International Business Machines Corporation 1996. All rights reserved.
Note to U.S. Government Users — Documentation related to restricted rights — Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.

Abstract

This redbook provides information about the key components of the IBM OS/2 Warp Server product. Following on the heels of OS/2 Warp Connect, the integrated OS/2 client operating system, OS/2 Warp Server combines the refreshed OS/2 Warp and LAN Server with a wealth of functional enhancements in TCP/IP, Remote Access Services (LAN Distance), systems management (SystemView), backup and recovery and advanced print function. Each service or function can be selectively installed, allowing users to customize OS/2 Warp Server to meet their specific needs. This redbook describes hints and workarounds for various installation scenarios.

The major enhancement to TCP/IP is the dynamic IP introduction. OS/2 Warp Server is the first product which has implemented Dynamic DNS (Domain Name System) together with DHCP (Dynamic Host Control Protocol). This redbook discusses the detail of this protocol and implementation on server and clients.

Remote Access Services is equivalent to the existing LAN Distance connection server product but with several enhancements. This redbook describes not only the enhancements but also the basics of remote access services.

This redbook intends to provide guidance on planning, installation and customization of the core components of OS/2 Warp Server. The components discussed in this redbook are the File and Print Sharing function with OS/2 and DOS/Windows/Windows 95 client, Adapter and Protocol Services, TCP/IP Services and Remote Access Services. For information on SystemView in OS/2 Warp Server, Backup and Recovery, and Advanced Print Services see the upcoming redbook, *Inside OS/2 Warp Server, Volume 2: Using SystemView, Backup/Recovery and Advanced Print* which is planned to be available in May/1996.

Readers are assumed to have some knowledge of OS/2 Warp, IBM OS/2 LAN Server 4.0 and basics of TCP/IP protocol and products.

(386 pages)

© Copyright IBM Corp. 1996

Contents

Abstract iii

Special Notices xix

Preface xxi
How This Document is Organized xxi
Related Publications xxii
International Technical Support Organization Publications xxii
How Customers Can Get Redbooks and Other ITSO Deliverables xxiii
How IBM Employees Can Get Redbooks and ITSO Deliverables xxiv
Acknowledgments xxv

Chapter 1. OS/2 Warp Server Version 4 Product Information 1
1.1 A Powerful Server 1
1.2 For Businesses of All Sizes 2
1.3 Broad Client Support 2
1.4 Enhanced TCP/IP Connectivity 2
1.5 Sophisticated Systems Management Made Easy 3
1.6 Carefree System Backup and Recovery 4
1.7 Remote Access 4
1.8 Advanced Print Functionality 5
1.9 Two Versions of OS/2 Warp Server 5

Chapter 2. File and Print Sharing Services 7
2.1 Overview 7
2.2 OS/2 Warp Server Domain Concept 10
2.3 Installation 10
Installation Considerations 13
2.4 Configuration 13
2.5 OS/2 Warp Server Tuning Assistant 15
Running the Tuning Assistant on a Requester 18
2.6 Sharing Resources with the Administration GUI 19
Sharing Files with the Administration GUI 20
Sharing Printers with the Administration GUI 23
Support for Thousands of Aliases 24
2.7 Other Methods of Sharing Resources 25
Sharing Resources from the Desktop 25
Sharing Resources from the Command Line 27
Sharing Resources from the Current Shares Window 27
2.8 Preparing the Server for Client Installation 28
2.9 Removing File and Print Sharing Services 32
2.10 OS/2 Warp Server Gateway Services 32
Overview and Concepts 33
NetWare File and Print Gateway Services 33
TCP/IP Services Interoperability 43

Chapter 3. File and Print Clients 49
3.1 What is a Requester? 50
3.2 OS/2 File and Print Client (OS/2 LAN Requester) 50
Installation 51
OS/2 Client Installation Considerations 57

© Copyright IBM Corp. 1996

Graphical User Interface 60
Connecting to Network Resources from the OS/2 File and Print Client . . . 62
3.3 DOS File and Print Client (DOS LAN Services) 64
New Features 65
Installation 66
Reduced Memory Requirements 77
Selecting the Redirector 79
Configuration 80
Graphical User Interface 80
3.4 Windows File and Print Client (DOS LAN Services Windows Support) . . 81
Installation 82
Configuration 83
Customizing your DOS LAN Services Windows GUI 83
DOS LAN Services Windows Shared Applications 86
DOS LAN Services General Hints and Tips 86
3.5 Windows 95 Client (DOS LAN Services for Windows 95) 87
Installation 88
Graphical User Interface 90
Accessing LAN Server Functions 90
The Windows 95 Network Neighborhood 91
Sharing Restrictions in non-NT Domains 91
3.6 Installing and Running DOS LAN Services on OS/2 91
Installing DOS LAN Services on OS/2 92
3.7 Connecting to Network Resources from DOS LAN Services 93
3.8 DOS LAN Services Logon Process 95
Local Logon 96
3.9 Sharing Requester Resources with the Peer Service 96
User Level Security 98
Peer Administration Considerations 100
Peer User Level Security APIs 101
3.10 Performance Tuning 103
3.11 DOS LAN Services Module Descriptions 104
3.12 DOS LAN Services Common Configuration Scenarios 105
Other Protocol 106
802.2 LAN Transport 106
TCPBEUI (Real-Mode) LAN Transport 106
TCPBEUI (Real-Mode) and IBM NetBEUI 106
TCPBEUI (Windows Protect-Mode) LAN Transport 107
TCPBEUI (Windows Protect-Mode) and IBM NetBEUI 107
TCPBEUI Configuration 107
DOS LAN Services TCPBEUI Utilities 107
3.13 NETWORK.INI Configuration File Parameters 110
NETWORK.INI Network Parameters 110
NETWORK.INI Messenger Parameters 113
NETWORK.INI Netpopup Parameter 113
NETWORK.INI Peer Parameters 113
Sample NETWORK.INI File 116
3.14 Password Coordination 116
Security Considerations 118
Installation 119
Configuration 119
Using Password Coordination 122

Chapter 4. Adapter and Protocol Services 125
4.1 Overview of Adapter and Protocol Services 125

New Features 125
Adapter and Protocol Support (LAPS) 126
Socket/Multiprotocol Transport Services (MPTS) 131
4.2 Installing Adapter and Protocol Services 133
Calculating Memory Requirements for Adapter and Protocol Services . . 137
4.3 Additional Configuration for Adapter and Protocol Services 142
Configuring Socket/MPTS 144
Removing Socket/MPTS Configuration 148
New Configuration Parameters for NetBEUI Protocol Driver 149
Configuring Adapter and Protocol Services for more than Four LAN Adapters 149
4.4 Useful Adapter and Protocol Services Applets 154
4.5 NetWare Requester for OS/2 157
Installing NetWare Requester Support on OS/2 Warp Server 159
4.6 NetWare NetBIOS Emulation 159
Configuring NetWare NetBIOS Emulation 161
Limitations When Using NetBIOS over IPX 165
Performance Considerations for IPXBEUI 165
4.7 DOS and Windows LAN Applications on OS/2 165
4.8 Removing Adapter and Protocol Services 166
4.9 Adapter and Protocol Support Related Publications 166

Chapter 5. TCP/IP Services 167
5.1 Overview of TCP/IP Services 167
New Functions of TCP/IP Services 168
Basic Functions and Services of TCP/IP 3.1 169
TCP/IP Services System Requirements 169
5.2 Installing TCP/IP Services 171
5.3 Additional Configuration for TCP/IP Services 173
5.4 A Short Introduction to Dynamic IP 197
Objectives and Customer Benefits of Dynamic IP 198
5.5 Dynamic Host Configuration Protocol (DHCP) 199
DHCP Initialization and Acquisition Process 199
DHCP Renewing, Rebinding and Rebooting Processes 201
DHCP Message Types and Message Format 202
5.6 Configuring an OS/2 DHCP Server 205
Configuring Site-Specific Options for OS/2 WARP TCP/IP 212
5.7 A Short Introduction to Cryptography 214
5.8 Dynamic Domain Name Services (DDNS) 216
DDNS Client to Server Interaction 217
DDNS Message Format and Resource Records 218
5.9 Configuring an OS/2 DDNS Server 222
Creating a New DDNS Server Configuration 223
Migrating an Existing DNS Configuration to Dynamic IP 226
Using a Dynamic DNS Server 227
5.10 Dynamic IP Client Support 228
OS/2 Dynamic IP Clients 228
DLS Dynamic IP Clients 233
5.11 Operational Scenario of Dynamic IP 233
Simple Dynamic IP Scenario 233
Complex Dynamic IP Scenario 237
Using Multiple Dynamic IP Servers 239
5.12 Interoperability with OEM and Legacy Hosts 239
Connecting Windows NT Clients to an OS/2 DHCP Server 239
Connecting Windows 95 Clients to an OS/2 DHCP Server 240

Connecting IBM Dynamic IP Clients to Windows NT DHCP Server 241
5.13 Accessing the Internet with OS/2 Warp Server 241
Internet Registration 242
Using IBM Internet Connection for OS/2 244
5.14 Expanding OS/2 Warp Server TCP/IP Capabilities 246
Network File System (NFS) Services 246
X Window System Server 248
IBM Internet Connection Server for OS/2 Warp 250
Enabling TCP/IP Services for Secure Firewall Access Using Socks 252
Developing Your Own TCP/IP Applications 254
Adding Wide Area Network (WAN) Connectivity to TCP/IP Services 255
5.15 Supporting DOS and Windows Applications with TCP/IP Services . . . 255
5.16 TCP/IP Client and Server Functions 256
5.17 Removing TCP/IP Services 258
5.18 TCP/IP Related Publications 258

Chapter 6. NetBIOS over TCP/IP (TCPBEUI) 259
6.1 Overview of NetBIOS Name Resolution over TCP/IP Network 259
6.2 NetBIOS over TCP/IP on OS/2 Warp Server 260
6.3 TCPBEUI Coexistence with NetBEUI 262
6.4 Reducing Broadcast Frames with TCPBEUI 264
Routing Extensions 264
Configuring TCPBEUI Routing Extensions 265
Name Cache and Name Discovery Algorithm 266
Storing NetBIOS Names on the Domain Nameserver 266
6.5 Configuring TCPBEUI to Support 1000 Clients 271
6.6 Using TCPBEUI with Dial-Up Connections 273
6.7 Performance Considerations for TCPBEUI 273
Tuning Considerations for TCPBEUI 274
6.8 Removing TCPBEUI Configuration 275
6.9 Using NetBIOS Name Server 275

Chapter 7. Remote Access Services 281
Functional Enhancements 281
7.1 Overview and Concepts 281
Remote Access Services Environments 283
Remote Access Services Clients 284
7.2 System Requirements 285
Remote Access Services Server 285
Remote Access Services Client 286
7.3 Setting Up the Remote Access Services 286
Installing the Remote Access Services 287
7.4 Configuring Remote Access Services 290
Open the Remote Access Services Settings Notebook 292
Configure the WAN Port 293
Configure the Modem 295
Configure the Bridge 298
Configure the Network Address 301
Configure the Answer Modes 303
Configure the Workstation 304
Configure the PhoneBook 305
Modifying MPTS for Remote Access Services Installation 311
Save the Configuration and Restart the Workstation 312
7.5 Setting Up an OS/2 Remote Access Services Client 313
Installation Considerations 313

Manual Remote Access Client Installation 315
Shuttling between LAN-Attached and Remote Workstation 316
7.6 Setting Up a Windows Remote Access Services Client 317
Limitations 317
Installation Considerations 318
7.7 Mobile File Sync and Remote Access Services 319
MFS Functions 320
Considerations 321
7.8 Deinstallation 322
7.9 Inactivity Timeout Feature 323
7.10 Adding Multiple Lines to the Remote Access Services 324
Open the Remote Access Services Settings Notebook 325
Configure the Modems 327
7.11 Implementing Security 331
Security Features 331
User Authentication Protocol 333
Security Policy Options 336
Additional Security Options 337
Protecting your Passphrase 339
Enabling the Remote Access Services Security Options 340
User Account Management 342
Security User Exit Package 352
Shared User Database 353
Security Database Tools 354
7.12 Application Considerations 356
LAN Server and LAN Requester 356
Communications Manager/2 357
NetWare 358
7.13 Understanding Bridging and Filtering 358
Remote Access Services Bridge Considerations 358
Segment Numbers 359
Hop Counts 360
Filtering 361
7.14 PIF Files for Uncertified Modems 363
7.15 Additional Information 364

Appendix A. Remote Access Services Internal Architecture 365
A.1 Remote Access Services and ANDIS 365
A.2 ANDIS Connection Request Flows 366
Remote Access Services Component Architecture 368
A.3 Relationship Between a Remote Workstation and the Connection Server 373

List of Abbreviations 377

Index 379

Figures

1. OS/2 Warp Server Product Components 1
2. IBM LAN Services Folder 7
3. Welcome to OS/2 Warp Server Installation 11
4. OS/2 Warp Server Component Installation 12
5. File and Print Sharing Services Feature Installation 12
6. OS/2 Warp Server Component Configuration 14
7. File and Print Sharing Services Feature Configuration 14
8. Server Hardware and Software Configuration Summary 15
9. Running the Tuning Assistant on a Requester 16
10. Configuration Warnings/Recommendations Screen 16
11. OS/2 Warp Server Component Requirements (Server) 17
12. Warnings or Recommendations Made 17
13. Updated Files Screen 18
14. Backup Files Confirmation Window 18
15. Running WSTUNE.EXE on a Requester 19
16. OS/2 Warp Server Administration Graphical User Interface 20
17. Directory Alias - Create notebook 21
18. Access Control Profile Does Not Exist Window 21
19. Defining an Access Control Profile for a Shared Directory 22
20. Propagate Access Control Profile to Subdirectories Window 22
21. Printer Alias - Create notebook 23
22. Defining an Access Control Profile for a Shared Printer 24
23. Network Extensions to Desktop Drive Object 25
24. Network Extensions to Desktop Printer Object 26
25. Commands to Share a Directory Resource from the Command Line . . 27
26. Sharing Resources from the Current Shares - Directories Window . . . 28
27. Where will Clients Access Installation? Window 29
28. File and Print Client Selection 29
29. Remote Installation Diskette Creation 30
30. File and Print Client Network Adapter Selection 30
31. Remote Installation Process 31
32. Remote Installation Status Window 31
33. Removing File and Print Sharing Services 32
34. NetWare File and Print Gateway Services Overview 34
35. Integrated Installation - NetWare File and Print Services 35
36. NetWare File and Print Services Folder 36
37. NetWare Installation and Configuration Program 36
38. NetWare Tools Network Option 38
39. NetWare Tools, Mapping a Drive 39
40. NetWare Tools, Capturing a Printer Port 40
41. TCP/IP File Sharing Gateway 44
42. TCP/IP Remote Printing Gateway 46
43. Internet Access via Shared COM Ports 47
44. Client Machines (Requesters) Supported By OS/2 Warp Server 49
45. OS/2 Warp Server Client Installation 51
46. OS/2 File and Print Client Installation 52
47. OS/2 File and Print Client Installation - Workstation Name 52
48. OS/2 File and Print Client Installation - Domain Name 53
49. Remote Access Client Installation 53
50. Remote Access Client Settings 54
51. TCP/IP Client Installation 54

© Copyright IBM Corp. 1996

52. TCP/IP Client Installation - DHCP/DDNS Support 55
53. System Management Client Installation 55
54. System Management Client Configuration 56
55. SystemView Software Distribution Configuration 56
56. OS/2 Warp Server Administration Graphical User Interface 61
57. Modifying your User Account Settings 62
58. Adding Logon Assignments 63
59. Adding Current Assignments 64
60. Windows Client Remote Installation - Client Selection 69
61. SystemView Windows Client Installation 70
62. SystemView Windows Client Configuration 70
63. SystemView for Windows Program Group 71
64. Windows Remote Access Client - Select Modem Type 72
65. Windows Remote Access Client - Specify Serial Port 72
66. Windows Remote Access Client - Specify Phone Number 73
67. Windows Remote Access Client - Select LAN Type 73
68. Windows Remote Access Client - Generate Logical Adapter Address . 74
69. Windows Remote Access Client - Enable NetWare Support 74
70. Sample DOS LAN Services Response File 77
71. Sample CONFIG.SYS for Maximum Memory Availability 78
72. Sample AUTOEXEC.BAT for Maximum Memory Availability 78
73. Sample NETWORK.INI for Maximum Memory Availability 78
74. DOS LAN Services Windows GUI 81
75. DOS LAN Services Windows Configuration Window 83
76. DOS LAN Services Windows GUI 84
77. Sample DOS LAN Services Customization File 84
78. Customized DOS LAN Services Windows GUI 85
79. DOS LAN Services in a Windows 95 Environment 88
80. DOS LAN Services for Windows 95 Installation 89
81. DOS LAN Services for Windows 95 Graphical User Interface 90
82. Changing Logon Drive Assignments 94
83. Sharing a Directory with DOS LAN Services Peer Services 97
84. Sharing a Printer with DOS LAN Services Peer Services 98
85. Sample DOS LAN Services NETWORK.INI File 116
86. Network SignON Coordinator - Signon Window 117
87. Network SignON Coordinator - Change Password Window 117
88. OS/2 Client NSC.INI File Example 119
89. NSC Exit for Changing Peer Passwords 120
90. NSC Exit for Changing Peer Passwords 123
91. Password Coordination - Main Folder 124
92. LAN Adapter and Protocol Support (LAPS) Overview 127
93. NDIS, OSI and IEEE Comparison 129
94. NDIS - Multiple Protocols 129
95. Socket/MPTS Overview 132
96. Initial Adapter and Protocol Services Configuration 134
97. Add Adapter Driver to Adapter and Protocol Services 135
98. Add Protocol Driver to Adapter and Protocol Services 136
99. Change Settings in Initial Adapter and Protocol Services Configuration 136
100. Adapter and Protocol Services - Configure Options 142
101. LAPS Configuration 143
102. TCP/IP Socket Access Configuration 144
103. TCP/IP Network Interface Configuration 145
104. TCP/IP Network Interface Configuration Using DHCP 146
105. Sockets Access Configuration 147
106. NetBIOS Configuration for Eight Adapters 150

107. NB64K Utility 154
108. NETPING Utility 156
109. ODI Stack 158
110. NetWare Requester for OS/2 159
111. IPXBEUI Coexistence 160
112. NetBIOS over IPX Protocol Stack 161
113. NetWare Requester Configuration Panel 162
114. CONFIG.SYS with NetBIOS over IPX Configured (Extract) 163
115. PROTOCOL.INI with NetBIOS over IPX Configured 164
116. IBMLAN.INI Configured for NetBIOS over IPX 164
117. NET.CFG File for NetWare NetBIOS Emulator 164
118. OS/2 Warp Server TCP/IP Services and Add-on Kits - Overview 168
119. OS/2 Warp Server Setup and Installation Menu 171
120. TCP/IP Services Installation - Dynamic IP Servers 171
121. TCP/IP Services Initial Configuration 172
122. TCP/IP Folder 174
123. IBM Internet Connection for OS/2 Folder 174
124. TCP/IP Services Configuration Notebook - Configure Network Interface Parameters 175
125. TCP/IP Services Network Interfaces - Advanced Options 176
126. TCP/IP Services Network Interfaces - Interface Configuration 177
127. TCP/IP Services Configuration Notebook - Configure Routing Information 178
128. TCP/IP Services Routing Page - Add Route Entry 179
129. TCP/IP Services Configuration Notebook - Configure LAN Name Resolution Services 180
130. TCP/IP Services Configuration Notebook - Configure Name Resolution Services 181
131. TCP/IP Services Hostnames Page 2 - Hosts Entry 182
132. TCP/IP Services Configuration Notebook - Configure Automatic Starting of Services 182
133. TCP/IP Services Configuration Notebook - Configure General Parameters 184
134. TCP/IP Services Configuration Notebook - Configure Server Security Page 1 185
135. TCP/IP Services Security Page 1 - FTP User Entry 186
136. TCP/IP Services Configuration Notebook - Configure Server Security Page 2 187
137. TCP/IP Services Security Page 2 - RHOSTS Entry 187
138. TCP/IP Services Configuration Notebook - Configure Servers for Applications 188
139. TCP/IP Services Configuration Notebook - Configure Printing Services 189
140. TCP/IP Services Configuration Notebook - Configure Mail for Ultimail or Mailing from NewsReader/2 190
141. TCP/IP Services Configuration Notebook - Configure POP for Ultimail or Mailing from NewsReader/2 191
142. TCP/IP Services Configuration Notebook - Configure Sendmail Parameters 192
143. TCP/IP Services Configuration Notebook - Configure Sendmail Parameters 193
144. TCP/IP Services Configuration Notebook - Configure SNMP Page 1 . . 194
145. TCP/IP Services Configuration Notebook - Configure SNMP Page 2 . . 195
146. TCP/IP Services SNMP Page 2 - SNMP Trap Destinations 195
147. TCP/IP Services SNMP Page 2 - SNMP Manager Access Authorization 196
148. DHCP Client State Transition Diagram 202

149. DHCP Message Format 203
150. DHCP Services Folder 206
151. DHCP Server Configuration Program 206
152. DHCP Server Configuration Program - Network Menu 208
153. OS/2 DHCP Server Program 210
154. DHCP Server Parameters 210
155. DHCP Server Configuration Program - Site-Specific Options 213
156. DDNS Message Format 219
157. DDNS Message Header Format 219
158. DDNS Resource Record Format 220
159. KEY Resource Record Format 220
160. SIG Resource Record Format 221
161. DDNS Services Folder 227
162. OS/2 DDNS Server Program 227
163. DHCP Client Monitor Program, Details View 229
164. DHCP Client Current Configuration 229
165. DDNS Client Configuration Program 231
166. Simple Dynamic IP Scenario 234
167. Complex Dynamic IP Scenario 238
168. Windows NT TCP/IP Configuration 240
169. Windows 95 TCP/IP Configuration 240
170. Windows NT DHCP Server Configuration 241
171. OS/2 Warp Server LAN and Internet Connectivity 242
172. Internet Account Registration 243
173. IBM Internet Customer Assistance Application 244
174. IBM Internet Dialer Application 245
175. IBM Internet Dialer Settings Notebook 245
176. IBM Internet Connection Login Panel 246
177. Network File System 247
178. OS/2 NFS Client Program 248
179. OS/2 NFS Server Program 248
180. X Window System Server 249
181. IBM Internet Connection Family 251
182. Internet Connection Server for OS/2 252
183. Firewall Operation 253
184. Firewall and Socks 254
185. TCP/IP DOS and Windows Application Support 256
186. NetBIOS, NetBIOS over TCP/IP and TCP/IP Structure 261
187. TCPBEUI Coexistence 263
188. LAPS Configuration Panel 264
189. IBMLAN.INI for Two NetBIOS Networks 264
190. TCPBEUI Configuration 265
191. Sample DNS Database File Before Adding Encoded NetBIOS Names . 268
192. Sample DNS Database File After Adding Encoded NetBIOS Names . . 270
193. TCPBEUI Configuration for 1000 Clients 272
194. How Server and Client Work with NetBIOS Name Server 276
195. Detail Flow of Server/Client to NetBIOS Name Server 277
196. Ideal Solution with DHCP/DDNS plus NBNS 278
197. Example of Remote System Manager for NTS NBNS 279
198. Remote Access Services Overview 282
199. Remote Access Services Configurations 284
200. Simple Remote Access Services Configuration 287
201. Remote Access Services Configuration/Installation Panel 288
202. Remote Access Services Configuration Action Items 290
203. LAN Distance Settings Window 293

204. Settings Window - Add Port 294
205. COM Port - Settings Window 294
206. Settings Window - Select Modems 295
207. Practical Peripherals FXSA Modem - Settings Window (Add Modem) . 296
208. Practical Peripherals FXSA Modem - Settings Window (Phone Number) 297
209. Practical Peripherals FXSA Modem - Settings Window (COM Port) . . 297
210. Practical Peripherals FXSA Modem - Settings Window (Assign Modem to a Port) 298
211. Settings Window (Bridge Section: Page 1 of 3) 299
212. Settings Window (Bridge Section: Page 2 of 3) 300
213. Settings Window (Bridge Section: Page 3 of 3) 301
214. Settings Window (Address Section: Page 1 of 2) 302
215. Settings Window (Answer Section: Change Settings) 303
216. Answer Criteria - Settings Window (Enable Answer) 304
217. Settings Window (Workstation Section) 305
218. PhoneBook, New Entry - Settings Window 306
219. PhoneBook, New Entry - Setting Window (Entry Section) 307
220. PhoneBook, New Entry - Settings Window 308
221. PhoneBook, New Entry - Settings Window (Modem Section) 309
222. PhoneBook, New Entry - Settings Window (Port Section) 310
223. PhoneBook, New Entry - Settings Window (Autostart Section) 311
224. Settings Window 311
225. LAPS Configure Workstation Window 312
226. Remote Access Client Selection 314
227. Remote Access Client Selection 314
228. Shuttle Option Window 316
229. Inactivity Timeout Option 324
230. Settings Notebook, Ports Tab 325
231. Adapter Type Selection Window 326
232. Settings Notebook, Ports Tab 326
233. Settings Notebook, Modems Tab 327
234. Select Modem Window 328
235. Ports Currently Assigned Window 328
236. Phone Number Window 329
237. Available Ports Window 329
238. Ports Currently Assigned Window 330
239. Settings Notebook, Modems Tab 330
240. LAN Distance Protocol Data Flow 334
241. Callback 338
242. Protecting Your Passphrase 340
243. Settings Notebook, Security Tab 341
244. LAN Distance Logon 342
245. Passphrase Expired 343
246. Change Passphrase 343
247. Personal Account Information (General Section) 344
248. Personal Account Information (Passphrase Section) 345
249. User Account Management Window (Account Section) 346
250. New - User Account Window (Type Section) 346
251. New - User Account Window (Passphrase Section) 347
252. New - User Account Window (Interval Section) 348
253. Change Logon Time Interval Window 349
254. New - User Account Window (Interval Section) 349
255. New - User Account Window (Addresses Section) 350
256. New - User Account Window (Callback Section) 351
257. User Account Management Window (Policy Section) 352

258. Interconnected LANs Using Remote Access Services 359
259. Setting Bridge Hop Counts 360
260. Simple LAN Communications 365
261. WAN Connection Management 366
262. ANDIS Connection Request Flows 367
263. ANDIS Architecture Overview 368
264. ANDIS Architecture Overview - Connection Manager 369
265. ANDIS Architecture Overview - Integrated Port Connection Manager . 370
266. ANDIS Architecture Overview - Source Routing Bridge 372
267. Connection Server and Remote Workstation Relationship - Token-Ring 373
268. Connection Server and Remote Workstation Relationship - Ethernet . 374

Tables

1. DOS LAN Services Installation Options Screen 1 67
2. DOS LAN Services Installation Options Screen 2 67
3. DOS LAN Services Remote Installation - Response File Keyword Reference 76
4. DOS LAN Services NET START Options and Initialization Process 80
5. DOS LAN Services WDLS.EXE Parameter Functions 85
6. Differences between the DOS LAN Services and OS/2 LAN Server APIs (Structure user_info_1) 102
7. Differences between the DOS LAN Services and OS/2 LAN Server APIs (Structure user_info_2) 102
8. Differences between the DOS LAN Services and OS/2 LAN Server APIs (PARMNUM) 103
9. DOS LAN Services Built In Groups 103
10. DOS LAN Services Module Descriptions 104
11. NETWORK.INI Network Section Parameter Values 110
12. NETWORK.INI Messenger Section Parameter Values 113
13. NETWORK.INI Netpopup Section Parameter Values 113
14. NETWORK.INI Peer Section Parameter Values 113
15. NSC.INI Configuration File Options 120
16. New Features of Adapter and Protocol Services 125
17. Adapter and Protocol Services Installation 134
18. Memory Calculations for NetBEUI 137
19. Memory Calculations for TCPBEUI 138
20. Memory Calculations for NetBIOS 139
21. Memory Calculations for IEEE 802.2 141
22. Adapter and Protocol Services Configuration 143
23. TCP/IP Network Interface Configuration 145
24. NetBIOS Interface Configuration for Socket Access 148
25. New Functions of TCP/IP Services 168
26. Fixed Disk Requirements for TCP/IP Services 169
27. Memory Requirements for TCP/IP Services 170
28. TCP/IP Services Initial Configuration 172
29. TCP/IP Services Configuration Notebook - Network Page 175
30. TCP/IP Services Network Interfaces - Advanced Options 176
31. TCP/IP Services Network Interfaces - Interface Configuration 177
32. TCP/IP Services Configuration Notebook - Routing Page 178
33. TCP/IP Services Routing Page - Add Route Entry 179
34. TCP/IP Services Configuration Notebook - Hostnames Page 1 180
35. TCP/IP Services Configuration Notebook - Hostnames Page 2 181
36. TCP/IP Services Hostnames Page 2 - Add Hosts Entry 182
37. TCP/IP Services Configuration Notebook - Autostart Page 183
38. TCP/IP Services Configuration Notebook - General Page 184
39. TCP/IP Services Configuration Notebook - Security Page 1 185
40. TCP/IP Services Security Page 1 - FTP User Entry 186
41. TCP/IP Services Configuration Notebook - Security Page 2 187
42. TCP/IP Services Security Page 2 - RHOSTS Entry 188
43. TCP/IP Services Configuration Notebook - Servers Page 188
44. TCP/IP Services Configuration Notebook - Printing Page 189
45. TCP/IP Services Configuration Notebook - Mail Page 1 190
46. TCP/IP Services Configuration Notebook - Mail Page 2 191
47. TCP/IP Services Configuration Notebook - Sendmail Page 1 192

© Copyright IBM Corp. 1996

48. TCP/IP Services Configuration Notebook - Sendmail Page 2 193
49. TCP/IP Services Configuration Notebook - SNMP Page 1 194
50. TCP/IP Services SNMP Page 2 - SNMP Trap Destinations 195
51. TCP/IP Services SNMP Page 2 - SNMP Manager Access Authorization 196
52. Files Modified by the TCP/IP Services Configuration Notebook 196
53. DHCP Server Configuration 199
54. DHCP Message Types 202
55. DHCP Message Fields 203
56. DHCP Options 204
57. DHCP Server Configuration - Predefined Resources Window 207
58. DHCP Server Configuration - Network Menu 208
59. DHCP Server Configuration - Server Parameters 211
60. DHCP Server Configuration - Site-Specific Options 213
61. DDNS Update Operations 219
62. KEY Resource Record Format 220
63. SIG Resource Record Format 221
64. OS/2 Warp Server TCP/IP Services 256
65. Remote Access Services File Changes 289
66. Remote Access Services Action List 291
67. Guidelines for Changing NetBIOS Timers 356
68. Remote Access Services Segment Configuration 359

Special Notices

This publication is intended to help IBM systems engineers and customers install and configure the core components of the IBM OS/2 Warp Server product. The information in this publication is not intended as the specification of any programming interfaces that are provided by IBM OS/2 Warp Server. See the PUBLICATIONS section of the IBM Programming Announcement for IBM OS/2 Warp Server for more information about what publications are considered to be product documentation.

References in this publication to IBM products, programs or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent program that does not infringe any of IBM's intellectual property rights may be used instead of the IBM product, program or service.

Information in this book was developed in conjunction with use of the equipment specified, and is limited in application to those specific hardware and software products and levels.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, 500 Columbus Avenue, Thornwood, NY 10594 USA.

The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The information about non-IBM (VENDOR) products in this manual has been supplied by the vendor and IBM assumes no responsibility for its accuracy or completeness. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

Any performance data contained in this document was determined in a controlled environment, and therefore, the results that may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environment.

Reference to PTF numbers that have not been released through the normal distribution process does not imply general availability. The purpose of including these reference numbers is to alert IBM customers to specific information relative to the implementation of the PTF when it becomes available to each customer according to the normal IBM PTF distribution process.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries:

AIX	AnyNet
APPN	AS/400
AT	CICS

© Copyright IBM Corp. 1996

CICS OS/2
DB2/2
IBM
LAN Distance
Library Reader
Nways
OS/400
Presentation Manager
PSF
RS/6000
ThinkPad
Workplace Shell

DB2
FFST/2
IMS
LANStreamer
MVS/ESA
OS/2
Portmaster
PS/2
PSF/6000
SystemView
WIN-OS/2

The following terms are trademarks of other companies:

C-bus is a trademark of Corollary, Inc.

PC Direct is a trademark of Ziff Communications Company and is used by IBM Corporation under license.

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

Microsoft, Windows, and the Windows 95 logo
are trademarks or registered trademarks of Microsoft Corporation.

Gopher	University of Minnesota
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IPX, NetWare, Novell	Novell, Inc.
Network File System, NFS	Sun Microsystems, Inc.
Lotus, Lotus Notes	Lotus Development Corporation
Motif, OSF	Open Software Foundation
Pentium	Intel Corporation
RSA	RSA Data Security, Inc.
Windows NT	Microsoft Corporation
X Window System	Massachusetts Institute of Technology (MIT)

Other trademarks are trademarks of their respective companies.

Preface

This redbook describes the core functions of the IBM OS/2 Warp Server product, based on the experiences of the systems engineers who participated in the ITSO, Austin Center, project.

The purpose of this redbook is to provide guidance on installing and configuring the core IBM OS/2 Warp Server components. This document does not describe the systems management, backup and restore, software distribution and advanced print services components of IBM OS/2 Warp Server. A separate redbook *Inside OS/2 Warp Server, Volume 2: Using SystemView, Backup/Recovery and Advanced Print* is planned to be available in May/1996. Knowledge of IBM OS/2 Warp and IBM OS/2 LAN Server 3.0 or 4.0, and an understanding of TCP/IP are assumed.

How This Document is Organized

The document is organized as follows:

- Chapter 1, "OS/2 Warp Server Version 4 Product Information"

  This chapter introduces a summary of OS/2 Warp Server.

- Chapter 2, "File and Print Sharing Services"

  The primary function of OS/2 Warp Server is to provide the ability to share resources. This chapter discusses how file and print resources are shared and how to tune your OS/2 Warp Server environment. In addition the chapter discusses how you may access the resources of other file sharing environments from an OS/2 Warp Server client by using OS/2 Warp Server as a gateway.

- Chapter 3, "File and Print Clients"

  OS/2 Warp Server provides support for all prevalent network clients. This chapter describes each client in detail and includes specific information on the new Windows 95 client.

- Chapter 4, "Adapter and Protocol Services"

  This chapter explains how to install and configure Adapter and Protocol Services and how to use the new and advanced features of this key component of OS/2 Warp Server.

- Chapter 5, "TCP/IP Services"

  This chapter describes the TCP/IP functions provided with OS/2 Warp Server and specifically concentrates on the new dynamic IP capabilities.

- Chapter 6, "NetBIOS over TCP/IP (TCPBEUI)"

  This chapter covers all of NetBIOS over TCP/IP functions or TCPBEUI issues in both static and dynamic IP environment.

- Chapter 7, "Remote Access Services"

  The Remote Access Services component of OS/2 Warp Server allows multiple concurrent remote OS/2 and Windows workstations to connect to a LAN and operate as if locally attached. This chapter discusses the installation, configuration and advanced features of Remote Access Services.

© Copyright IBM Corp. 1996

- Appendix A, "Remote Access Services Internal Architecture"

  This appendix includes some information on the internal design and architecture of the Remote Access Services. You do not require a detailed understanding of the internal structure of the Remote Access Services to install and use it. The information presented here can prove valuable to people who are using Remote Access Services in an advanced environment.

Related Publications

The publications listed in this section are considered particularly suitable for the topics covered in this document.

- *OS/2 Warp Server Version 4 Easy Start*, S25H-8003
- *OS/2 Warp Server Version 4 Up and Running!*, S25H-8004
- *OS/2 LAN Server Network Administrator Reference, Volume 1: Planning, Installation, and Configuration*, S10H-9680
- *OS/2 LAN Server Network Administrator Reference, Volume 2: Performance Tuning*, S10H-9681
- *OS/2 LAN Server Network Administrator Reference, Volume 3: Network Administrator Tasks*, S10H-9682
- *LAN Server Command and Utilities*, S10H-9686
- *IBM LAN Distance Remote Guide*, S52G-8393
- *IBM LAN Distance Advanced Guide*, S52G-8394
- *IBM Multi-Protocol Transport - AnyNet for OS/2: Configuration Guide*, S25H-7867
- *LAN Technical Reference IEEE 802.2 and NETBIOS APIs*, SC30-3587
- *TCP/IP for OS/2 V2.0 Installation and Administration*, SC31-6075
- *IBM TCP/IP Version 2.0 for OS/2 Domain Name Server Guide*, SC31-7174

The following list of books are available from book stores and are useful for understanding TCP/IP and Internet:

- *Internetworking with TCP/IP Volume 1* by Douglas E. Comer
- *The Whole Internet User's Guide and Catalog* by Ed Krol
- *The Internet for Dummies* by John R. Levine and Carol Baroudi
- *Your OS/2 Warp Internet Connection* by Deborah Morrison

International Technical Support Organization Publications

- *Inside OS/2 Warp Server, Volume 2: Using SystemView, Backup/Recovery and Advanced Print*, SG24-4702 (to be available in May/96)
- *Inside OS/2 LAN Server 4.0*, SG24-4428
- *OS/2 Warp Generation, Volume 1: OS/2 Warp Version 3, OS/2 Warp with Windows and BonusPak*, SG24-4552
- *OS/2 Warp Generation, Volume 2: Exploring LAN Connectivity with OS/2 Warp Connect*, GG24-4505
- *TCP/IP V2.0 for OS/2 Installation and Interoperability*, GG24-3531

- *Understanding IBM OS/2 LAN Server Performance Tuning*, GG24-4430
- *NetWare Client for OS/2 Installation and Configuration*, GG24-3891-01
- *IBM LAN Distance Version 1.1 Configuration and Customization Guide*, GG24-4158-01

A complete list of International Technical Support Organization redbooks, with a brief description of each, may be found in:

International Technical Support Organization Bibliography of Redbooks, GG24-3070.

To get a catalog of ITSO redbooks online, VNET users may type:

```
TOOLS SENDTO WTSCPOK TOOLS REDBOOKS GET REDBOOKS CATALOG
```

A listing of all redbooks, sorted by category, may also be found on MKTTOOLS as ITSOCAT TXT. This package is updated monthly.

How Customers Can Get Redbooks and Other ITSO Deliverables

Customers may request ITSO deliverables (redbooks, BookManager BOOKs, and CD-ROMs) and information about redbooks, workshops, and residencies in the following ways:

- **IBMLINK**

  Registered customers have access to PUBORDER to order hardcopy, to REDPRINT to obtain BookManager BOOKs

- **IBM Bookshop** — send orders to:

  usib6fpl@ibmmail.com (USA)
  bookshop@dk.ibm.com (Outside USA)

- **Telephone orders**

  1-800-879-2755 (USA)
  354-9408 (Australia)
  359-2-731076 (Bulgaria)
  42-2-67106-250 (Czech Republic)
  593-2-5651-00 (Ecuador)
  03-69-78901 (Israel)
  905-627-1163 (Mexico)
  064-4-57659-36 (New Zealand)
  027-011-320-9299 (South Africa)

  0256-478166 (UK)
  32-2-225-3738 (Belgium)
  1-800-IBM-CALL (Canada)
  45-934545 (Denmark)
  01805-5090 (Germany)
  0462-73-6669 (Japan)
  31-20513-5100 (Netherlands)
  507-639977 (Panama)

- **Mail Orders** — send orders to:

  IBM Publications
  P.O. Box 9046
  Boulder, CO 80301-9191
  USA

  IBM Direct Services
  Sortemosevej 21,
  3450 Allerod
  Denmark

- **Fax** — send orders to:

  1-800-445-9269 (USA)
  32-2-225-3478 (Belgium)
  905-316-7210 (Canada)
  593-2-5651-45 (Ecuador)
  03-69-59985 (Israel)
  31-20513-3296 (Netherlands)

  0256-843173 (UK)
  359-2-730235 (Bulgaria)
  42-2-67106-402 (Czech Republic)
  07032-15-3300 (Germany)
  0462-73-7313 (Japan)
  064-4-57659-16 (New Zealand)

507-693604 (Panama) 027-011-320-9113 (South Africa)

- **1-800-IBM-4FAX (USA only)** — ask for:

  Index # 4421 Abstracts of new redbooks
  Index # 4422 IBM redbooks
  Index # 4420 Redbooks for last six months

- **Direct Services**

  Send note to softwareshop@vnet.ibm.com

- **Redbooks Home Page on the World Wide Web**

  http://www.redbooks.ibm.com/redbooks

- **E-mail (Internet)**

  Send note to redbook@vnet.ibm.com

- **Internet Listserver**

  With an Internet E-mail address, anyone can subscribe to an IBM Announcement Listserver. To initiate the service, send an E-mail note to announce@webster.ibmlink.ibm.com with the keyword subscribe in the body of the note (leave the subject line blank). A category form and detailed instructions will be sent to you.

How IBM Employees Can Get Redbooks and ITSO Deliverables

Employees may request ITSO deliverables (redbooks, BookManager BOOKs, and CD-ROMs) and information about redbooks, workshops, and residencies in the following ways:

- **PUBORDER** — to order hardcopies in USA

- **GOPHER link to the Internet**

  Type GOPHER
  Select IBM GOPHER SERVERS
  Select ITSO GOPHER SERVER for Redbooks

- **Tools disks**

  To get LIST3820s of redbooks, type one of the following commands:

  ```
  TOOLS SENDTO EHONE4 TOOLS2 REDPRINT GET GG24xxxx PACKAGE
  TOOLS SENDTO CANVM2 TOOLS REDPRINT GET GG24xxxx PACKAGE (Canadian users only)
  ```

  To get lists of redbooks:

  ```
  TOOLS SENDTO WTSCPOK TOOLS REDBOOKS GET REDBOOKS CATALOG
  TOOLS SENDTO USDIST MKTTOOLS MKTTOOLS GET ITSOCAT TXT
  TOOLS SENDTO USDIST MKTTOOLS MKTTOOLS GET LISTSERV PACKAGE
  ```

  To register for information on workshops, residencies, and redbooks:

  ```
  TOOLS SENDTO WTSCPOK TOOLS ZDISK GET ITSOREGI 1996
  ```

  For a list of product area specialists in the ITSO:

  ```
  TOOLS SENDTO WTSCPOK TOOLS ZDISK GET ORGCARD PACKAGE
  ```

- **Redbooks Home Page on the World Wide Web**

  http://w3.itso.ibm.com/redbooks/redbooks.html

- **ITSO4USA category on INEWS**

- **IBM Bookshop** — send orders to:

  USIB6FPL at IBMMAIL or DKIBMBSH at IBMMAIL

- **Internet Listserver**

  With an Internet E-mail address, anyone can subscribe to an IBM Announcement Listserver. To initiate the service, send an E-mail note to announce@webster.ibmlink.ibm.com with the keyword subscribe in the body of the note (leave the subject line blank). A category form and detailed instructions will be sent to you.

Acknowledgments

This project was designed and managed by:

Oscar Cepeda	ITSO, Austin Center
Toshi Shimizu	ITSO, Austin Center

The authors of this document are as follows:

Geraldo Macedo	IBM Brazil
Martin Murhammer	IBM Austria
Indran Naick	IBM South Africa
Emmanuel Odier	IBM France
Hermann Pauli	IBM Germany
Alain Rykaert	IBM Belgium
Andrew Taylor	IBM United Kingdom
Enrique Testini	IBM Italy
Colin Vernon	IBM United Kingdom
Uwe Zimmermann	ITSO, Austin Center

This publication is the result of a residency conducted at the International Technical Support Organization, Austin Center.

Thanks to the following people for their invaluable advice and help provided in the production of this document:

- IBM Austin

  Paul Carson
  Gary Hunt
  Don Mulvey
  Jim Pickering
  Doug Spelce
  Steve Tipton
  Galen Watson
  Ken Whitfield

- IBM Raleigh

  Bryan Frey
  Danielle Moore
  Glenn Stump
  Wendy White

- Other companies

  Brice Bartek, Network TeleSystems, Inc.
  Linda De Los Reyes, RSA Inc.

Fold and Tape **Please do not staple** Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM International Technical Support Organization
Department JN9B, Building 045
Internal Zip 2834
11400 BURNET ROAD
AUSTIN TX
USA 78758-3493

Fold and Tape **Please do not staple** Fold and Tape

ITSO Technical Bulletin Evaluation RED000

Inside OS/2 Warp Server, Volume 1:
Exploring the Core Components

Publication No. SG24-4602-00

Your feedback is very important to help us maintain the quality of ITSO Bulletins. **Please fill out this questionnaire and return it using one of the following methods:**

- Mail it to the address on the back (postage paid in U.S. only)
- Give it to an IBM marketing representative for mailing
- Fax it to: Your International Access Code + 1 914 432 8246
- Send a note to REDBOOK@VNET.IBM.COM

Please rate on a scale of 1 to 5 the subjects below.
(1 = very good, 2 = good, 3 = average, 4 = poor, 5 = very poor)

Overall Satisfaction	___		
Organization of the book	___	Grammar/punctuation/spelling	___
Accuracy of the information	___	Ease of reading and understanding	___
Relevance of the information	___	Ease of finding information	___
Completeness of the information	___	Level of technical detail	___
Value of illustrations	___	Print quality	___

Please answer the following questions:

a) If you are an employee of IBM or its subsidiaries:
   Do you provide billable services for 20% or more of your time? Yes___ No___
   Are you in a Services Organization? Yes___ No___

b) Are you working in the USA? Yes___ No___

c) Was the Bulletin published in time for your needs? Yes___ No___

d) Did this Bulletin meet your needs? Yes___ No___
   If no, please explain:

_____

_____

What other topics would you like to see in this Bulletin?

_____

_____

What other Technical Bulletins would you like to see published?

_____

Comments/Suggestions: **(THANK YOU FOR YOUR FEEDBACK!)**

_____ _____
Name Address

_____ _____
Company or Organization

_____ _____
Phone No.

Chapter 1. OS/2 Warp Server Version 4 Product Information

OS/2 Warp Server, Version 4, is IBM's one-box server operating system solution for customers ranging from small and medium-sized businesses to large enterprises. It combines a foundation for application serving with integrated file and print sharing, and offers an easy-to-use graphical user interface for drag-and-drop administration.

Following on the heels of OS/2 Warp Connect, IBM's network client operating system, OS/2 Warp Server combines the market-proven quality of OS/2 Warp and LAN Server 4.0 with a wealth of functional enhancements in systems management, backup and recovery, remote access, enhanced TCP/IP support, advanced print function, and LAN Internet access. All services are integrated into the product, eliminating the time and cost of having to separately install each component. However, services such as file and print can be selectively installed, allowing users to customize OS/2 Warp Server to meet their specific needs. The installation procedure also includes auto-detection of devices such as network interface cards.

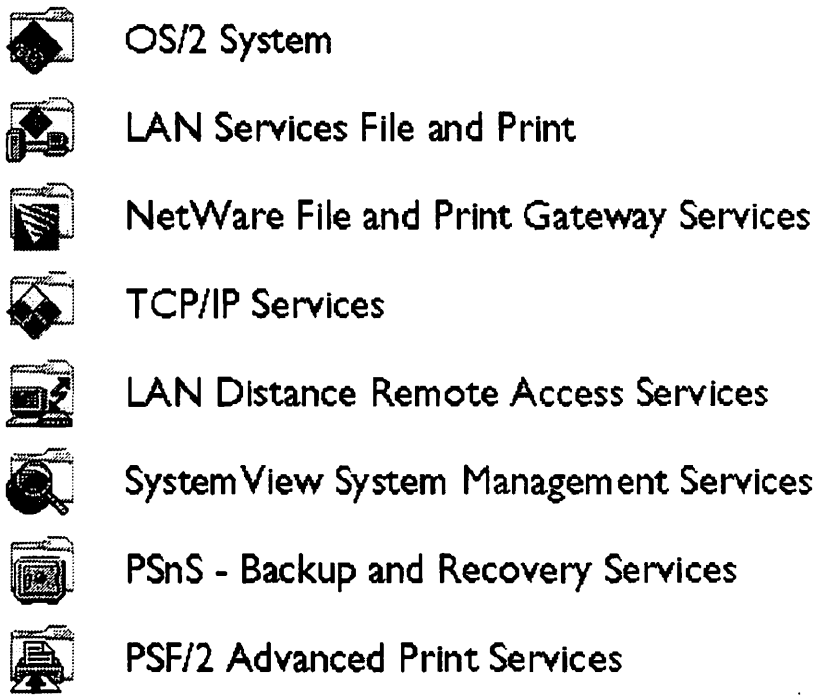

OS/2 System
LAN Services File and Print
NetWare File and Print Gateway Services
TCP/IP Services
LAN Distance Remote Access Services
SystemView System Management Services
PSnS - Backup and Recovery Services
PSF/2 Advanced Print Services

Figure 1. OS/2 Warp Server Product Components

1.1 A Powerful Server

OS/2 Warp Server inherits from LAN Server 4.0 a sophisticated set of network capabilities, including an easy-to-use drag-and-drop administration model which allows network administrators and resellers to quickly install, set up, configure and manage a network. It offers tight security that is flexible enough to be customized to the needs of any business by assigning various privileges down to specific files on the server. OS/2 Warp Server also uses a powerful high performance file system and includes a NetWare migration utility that will allow

© Copyright IBM Corp. 1996

an organization to migrate NetWare 2.x and 3.x users and information onto an OS/2 Warp Server environment using a graphical user interface.

OS/2 Warp Server possesses the same 32-bit, preemptive multitasking capabilities of IBM's powerful and battle-tested OS/2 Warp operating system, and comes Internet-ready with IBM's popular Internet Access Kit and WebExplorer. It offers reliable crash protection, runs OS/2 and DOS applications and contains IBM's WIN-OS/2 code, which provides support for 16- and 32-bit Windows applications.

1.2 For Businesses of All Sizes

With sophisticated, easy-to-use networking components on a powerful operating system platform, OS/2 Warp Server will appeal to a diverse set of market segments, from small and medium sized businesses to departmental corporate workgroups to large businesses and institutions. Resellers and VARs are also an important target audience for OS/2 Warp Server. Not only do they stand to benefit from selling a complete business solution to such a broad set of users, but their job is made easier with OS/2 Warp Server's outstanding system management capabilities.

1.3 Broad Client Support

OS/2 Warp Server supports all prevalent network clients, including OS/2 Warp and OS/2 Warp Connect, DOS, Windows 3.x, Windows NT Workstation, Windows for Workgroups and Windows 95. Macintosh clients are supported via IBM's LAN Server for Macintosh add-on product and AIX clients are supported via IBM's PC Connection product, both available separately. OS/2 Warp Server is backward compatible with previous IBM LAN Server clients. This will allow OS/2 Warp Server servers to be incrementally added to an existing LAN Server network and will provide the customer with complete compatibility between systems. OS/2 Warp Server also supports gateway functionality to Novell NetWare and Microsoft NT and LAN Manager servers, allowing OS/2 Warp Server clients to access non-OS/2 Warp Server resources.

1.4 Enhanced TCP/IP Connectivity

Equipped with new features such as Dynamic Host Configuration Protocol (DHCP) and Dynamic Domain Name Services (DDNS) servers and a NetBIOS over TCP/IP implementation that allows customers to connect up to a thousand client workstations, OS/2 Warp Server can share its power with systems in a heterogeneous environment. As TCP/IP is becoming more and more popular, OS/2 Warp Server delivers exciting new functions to the world of TCP/IP users.

Network administrators face a host of challenges building and maintaining their TCP/IP networks. Typically, they must assign IP (internet protocol) addresses, host names, and other network information at individual computers. This forces them to track changes every time a computer is either added, removed or relocated in the network. Users or administrators must also manually configure computers for network access. These tasks are time-consuming, error prone, and can disrupt network operations. IBM has addressed these challenges with a new networking technology called Dynamic IP.

IBM is introducing Dynamic IP in OS/2 Warp Server. Dynamic IP implements a true TCP/IP *plug-and-go* network solution, greatly simplifying both IP network access and IP network administration. Furthermore, Dynamic IP is well-suited for networking mobile hosts and is fully compatible and interoperable with existing IP network hosts and routers.

Dynamic IP is the integration of the Dynamic Host Configuration Protocol (DHCP) and Dynamic Domain Naming System (DDNS). Both DHCP and Dynamic DNS are new features to OS/2 Warp Server, and Dynamic DNS is a first in the industry.

DHCP and DDNS are complementary open networking standards developed by the IETF (Internet Engineering Task Force) which assures compatibility with clients and servers on other operating systems, including UNIX, Windows NT, and Windows 95. Each protocol implements half of the TCP/IP *plug-and-go* network solution. The DHCP protocol centralizes and automates the configuration of IP hosts, including IP addresses, while the Dynamic DNS protocols automatically record the association between IP hosts and their DHCP-assigned addresses.

Using DHCP and DDNS, a host automatically configures itself for network access wherever it *plugs-in* to the IP network. That host can then be located and accessed using its permanent, unique DNS host name. Mobile hosts, for example, can therefore freely move about a network without knowledge of the local IP network addresses or services and without end-user or administrator intervention.

The OS/2 Warp Server software package includes a Dynamic IP client, a DHCP server, and a Dynamic DNS Server. The Dynamic IP client consists of both a DHCP and a Dynamic DNS client component. The DHCP client may be configured to operate as a simple DHCP client or as a Dynamic IP client, integrating Dynamic DNS client services with the DHCP client.

The Dynamic DNS server is a superset of the industry-standard *BIND* DNS server and may be configured to operate as a traditional static DNS server or a new Dynamic DNS server, or both.

The capability of transmitting the NetBIOS application protocol over TCP/IP networks enables OS/2 Warp Server to be accessed across geographically dispersed system environments as well as in local area networks (LANs). This function is also based on open standards (RFCs 1001/1002) to ensure compatibility with a wide range of clients and servers using NetBIOS over TCP/IP.

1.5 Sophisticated Systems Management Made Easy

To address the challenges faced by today's network administrators, OS/2 Warp Server will contain systems management features which ensure a high degree of performance and reliability. Administrators will be able to remotely manage computers across the network, allowing them to quickly address network issues by monitoring or even taking control of any computer on a LAN without leaving their desk.

OS/2 Warp Server provides a software and hardware discovery feature for system administrators, giving network supervisors the ability to determine the

exact components of any PC on the network. System administrators will be able to determine such components as software titles, version number of programs, type of configuration, type and size of hard disk drive, amount of system memory and network interface card. This will help administrators identify software upgrades, detect system incompatibilities and determine the need for hardware upgrade components. By having the ability to do all of this without leaving their desks, administrators will be able to manage their systems much more easily and efficiently, reducing the cost of LAN management.

As a preventive measure, on-screen alerts built into OS/2 Warp Server will warn administrators of predictive hardware failures such as low disk space and exceeding the CPU threshold. This is an added benefit to resellers because it helps them avoid potential customer satisfaction problems.

Details of the system management and software distribution features of OS/2 Warp Server may be found in *Inside OS/2 Warp Server, Volume 2: Using SystemView, Backup/Recovery and Advanced Print* which is planned to be available in May 1996.

1.6 Carefree System Backup and Recovery

Reliable protection from data loss is vital for any business employing a network. IBM has implemented a comprehensive backup and recovery system in OS/2 Warp Server that eliminates the worry. Utilizing object-oriented administration and an intuitive interface, OS/2 Warp Server offers an easy-to-use, yet sophisticated, backup solution.

OS/2 Warp Server users will be able to schedule full or partial data backups to a variety of media formats including diskette, tape and optical drives. An advanced disaster recovery feature is included that will allow a business to recover vital data, even in the event of a complete server hard disk crash. Users will also have the unique ability to load tape backups and restore information to the network without loading the core operating system, allowing them to easily and painlessly recover data and get their business up and running again very quickly.

This integrated backup facility is also compatible with IBM's Adstar Distributed Storage Manager (ADSM), which allows users to manage data centrally on a variety of IBM and non-IBM platforms, including DEC, Apple, Hewlett-Packard, Sun, Novell and Windows, as well as IBM's MVS, VM, VSE, AIX and AS/400 environments. This scalability across platforms protects investments and creates an efficient heterogeneous operating environment.

1.7 Remote Access

Remote connectivity is a need for businesses of all sizes today, and OS/2 Warp Server features a full set of remote access capabilities. Organizations ranging from small businesses with two sites across town to multinational corporations can now quickly access vital information via this integrated remote functionality.

With OS/2 Warp Server's remote node capability, users are able to log onto the network, upload and download data and print documents to other facilities. Offices will be able to quickly share information by linking to their corporate

network and other sites via a high speed modem line, X.25 or ISDN. Mobile users can connect to the office as though they were sitting at their desks.

In addition, OS/2 Warp Server's remote control feature reduces the cost of support. A system administrator or reseller will actually be able to see what the user sees, extending the ability to reach out and view, troubleshoot and solve network issues from across town or from thousands of miles away.

1.8 Advanced Print Functionality

Printing over the network is an important task for organizations of all sizes. OS/2 Warp Server includes new printing enhancements that will solve various needs for a variety of customers. With OS/2 Warp Server's postscript printer emulation, users are able to send postscript documents to non-PostScript laser printers such as Hewlett-Packard and LexMark, saving both time and money.

OS/2 Warp Server also has advanced printer functionality that is compatible with high speed host printers in a mainframe connected environment. This compatibility will greatly assist organizations by protecting their investments in high-capacity host printers. A corporate customer can easily introduce OS/2 Warp Server into the network and configure this advanced business network solution to drive 300 page per minute printers, again saving much time and money.

Details of the advanced print features of OS/2 Warp Server may be found in *Inside OS/2 Warp Server, Volume 2: Using SystemView, Backup/Recovery and Advanced Print* which is planned to be available in May 1996.

1.9 Two Versions of OS/2 Warp Server

OS/2 Warp Server is available in two versions:

- OS/2 Warp Server Version 4, which includes all of the features already mentioned and supports approximately 120 users for file and print sharing and 1,000 users for application serving.
- OS/2 Warp Server Advanced Version 4, which includes the same features, plus fault tolerance, enhanced Pentium optimization and user disk limits. The Advanced version includes 32-bit High Performance File System for higher performance file and print sharing and Lotus Notes usage, and supports up to 1,000 users on a single server.

Chapter 2. File and Print Sharing Services

The File and Print Sharing Services component of OS/2 Warp Server is a local area network (LAN) application which is functionally equivalent to OS/2 LAN Server 4.0 with Service Pack IP08152 applied. It allows you to share hardware and software resources that are located on a server workstation.

You may share the directories (and the applications and files contained in them) and the printers and serial devices (such as a modem or plotter) that are connected to the server workstation. These shared resources are also referred to as network resources.

From a workstation, after you have connected to a network resource, you may use that resource in the same way you use local resources.

Note: DOS and Windows clients may not access shared serial devices unless they are redirected to LPT ports for output only (serially attached printers and plotters for example).

2.1 Overview

When you open the IBM LAN Services folder, the following File and Print Sharing Services functions are available.

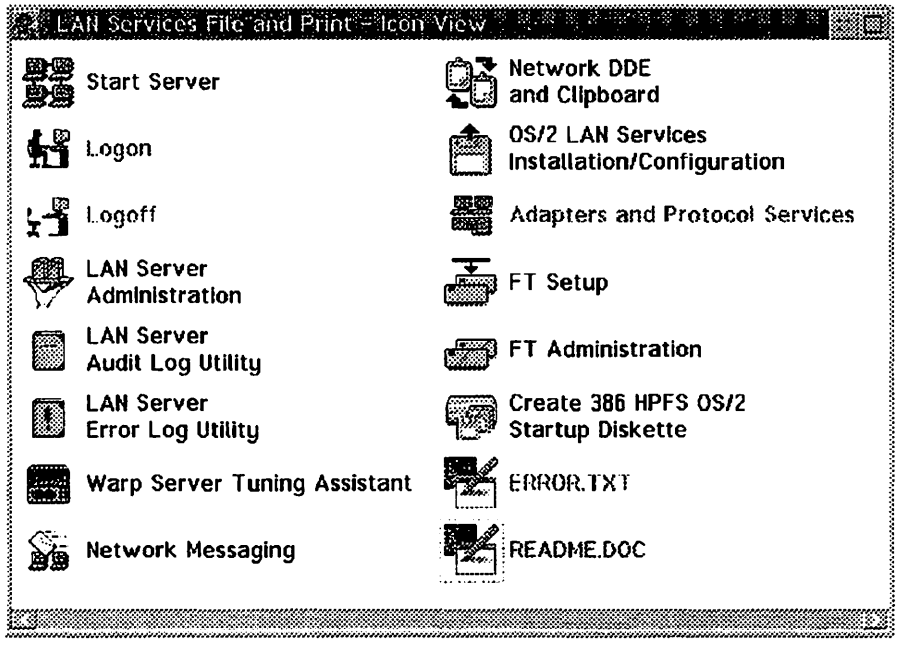


Figure 2. IBM LAN Services Folder

Each object, as shown in Figure 2, represents a specific function:

- **Start Server**

  Select this object to start the File and Print Sharing Services on the server workstation if you did not select to automatically start the server using the changes applied to STARTUP.CMD as part of the installation process.

- **Logon**

© Copyright IBM Corp. 1996

Allows you to perform domain logon and local logon (for subsystems requiring local verification). OS/2 Warp Server does not require local logon.

- **Logoff**

  Allows you to log off the domain. Make sure all network applications are closed before logging off otherwise you will need to confirm that you wish to terminate each individual network application and all associated connections.

- **LAN Server Administration**

  Allows you to administer a network running OS/2 Warp Server. Whether or not you are already familiar with manipulating objects in OS/2 2.x you will find it very easy to administer your OS/2 Warp Server environment by simply dragging and dropping objects to manage users, groups, and shared resources. We take a look at the OS/2 Warp Server Administration GUI in 2.6, "Sharing Resources with the Administration GUI" on page 19.

- **LAN Server Audit Log Utility**

  This is where you look to view OS/2 Warp Server events and other events that you have defined to be logged. You will notice that any changes you make to the sort order will be saved and retrieved every time you view the Audit Log. This is an enhancement to LAN Server 4.0 (prior to IP08152).

- **LAN Server Error Log Utility**

  If you experience problems starting your OS/2 Warp Server, or see any errors during operation, then this utility will identify the problem and provide advice on what you should do to resolve it. You will notice that any changes you make to the sort order will be saved and retrieved every time you view the Error Log. This is an enhancement to LAN Server 4.0 (prior to IP08152).

- **IBM OS/2 Warp Server Tuning Assistant**

  Provides automatic tuning and configuration of your OS/2 Warp Server. We will look at this feature in detail in 2.5, "OS/2 Warp Server Tuning Assistant" on page 15.

- **Network Messaging**

  Selecting this object enables you to send messages to, and receive messages from, users on the network.

- **Network DDE and Clipboard**

  You can use this function to cut and paste data into other applications on the network using dynamic data exchange (DDE) and Clipboard functions.

- **OS/2 LAN Services Installation/Configuration**

  You would use this function to reinstall, reconfigure or remove the File and Print Sharing Services function from the local workstation. It also provides you with the option to create response files (for CID installation). See Figure 33 on page 32.

- **Adapters and Protocol Services**

  Allows you to configure PROTOCOL.INI file parameters for the protocol(s) and NDIS driver(s) on the workstation. Refer to the online MPTS/2 books and Chapter 4, "Adapter and Protocol Services" on page 125 for further information.

Note: When modifying the MPTS/2 configuration you *must* use this object. Using the MPTS/2 object on the OS/2 Warp Server Desktop will not update the netx statement(s) in the File and Print Sharing Services configuration file (IBMLAN.INI).

- **Fault Tolerance Setup**

  Provides the FTSETUP utility to set up Fault Tolerance on the network for the first time. OS/2 Warp Server File and Print Sharing Services provides the following fault tolerance features:

  - Drive mirroring

    The ability to duplicate a single logical drive or volume on two partitions which are on different disks. This protects you against a single drive failure.

  - Drive duplexing

    Providing further protection by imposing a restriction that the two disks on which the partitions reside are controlled by two different disk controllers. This protects you against both single drive failure and single disk controller failure.

- **Fault Tolerance Administration**

  Provides the FTADMIN utility to manage Fault Tolerance on the network.

  Notes:

  1. Fault Tolerance functions are *not* available with the OS/2 Warp Server Entry package.
  2. Fault Tolerance functions are not automatically installed with File and Print Sharing Services. You must specify that you wish to install them by selecting the appropriate check box as shown in Figure 5 on page 12.

- **Create 386 HPFS OS/2 Startup Diskette**

  The OS/2 Warp Server Advanced package uses a highly optimized derivative of the OS/2 Warp high performance file system (HPFS). When a partition is formatted for 386 HPFS you will not be able to access files on that partition unless the 386 HPFS installable file system (IFS) driver is loaded. Therefore, to access a system which does not have a valid CONFIG.SYS file you need to boot from the OS/2 Warp Installation Diskette and a backup copy of the OS/2 Warp Diskette 1 which has been modified by this utility to include the 386 HPFS file system driver.

  Note: If you experience problems with the \IBMLAN\NETPROG\WSBOOT.CMD utility, check the volume label of your OS/2 Warp Server CD-ROM 1. If the volume label is WARP_SERVER (with underscore '_'), please alter line 54 of the the REXX command file appropriately.

IBMRAID.ADD

For server machines based on RAID technology, be sure to have the IBMRAID.ADD driver copied onto the modified OS/2 Warp Diskette 1. Also, the following line must be appended as line one to the CONFIG.SYS file:

```
BASEDEV=IBMRAID.ADD
```

For more information, see "Installation Considerations" on page 13.

As previously mentioned, OS/2 Warp Server shares much in common with the LAN Server 4.0 package. For a thorough discussion of the above features please refer to the redbook *Inside OS/2 LAN Server 4.0*.

In this chapter we will cover in detail the tasks that you are likely to want more information on as you start sharing resources in an OS/2 Warp Server environment.

2.2 OS/2 Warp Server Domain Concept

Before we take a look at the File and Print Sharing Services provided with OS/2 Warp Server it is important that you understand the concept of a *domain*. It is very likely that you will want to share the resources located on more than one server workstation in your OS/2 Warp Server environment.

A domain is a named network consisting of a group of workstations linked together to share resources such as directories, printers, modems and plotters. You logon to an OS/2 Warp Server domain and gain access to shared resources which may be located on a number of server workstations in the domain. To the user it appears as though they are connected to a single server and they are unaware that they are accessing resources which may be located on different servers. They are presented with a *single system image*.

Each domain consists of the following types of workstations:

- There is always one, and only one, primary server workstation called the *domain controller* that maintains the master copies of the user and group definitions. The domain controller also has details of access permissions that users and groups have to use shared resources and also how they appear to them when they log on.

  The domain controller processes user's logon requests and may also share it's own resources.

- Optionally, additional server workstations may be installed to provide shared resources and to serve as backup domain controllers. Backup domain controllers support the domain controller in processing logon requests and can take over the role of the domain controller should it fail.

- Requesters, from which users can access shared resources on the server workstations. We look at the various requesters that may be used with OS/2 Warp Server in Chapter 3, "File and Print Clients" on page 49.

This is a high level overview of domains. For a more detailed discussion please refer to the OS/2 Warp Server publication named *Up & Running!*.

For an in-depth explanation of the backup domain controller's function in a domain please refer to the redbook *Inside OS/2 LAN Server 4.0*.

2.3 Installation

File and Print Sharing Services is obviously the key component of OS/2 Warp Server and is therefore presented as the first component available to install as shown in Figure 4 on page 12.

Detailed step by step installation instructions are provided in the OS/2 Warp Server *Easy Start* publication. Therefore, we will only look at certain aspects of

the File and Print Sharing Services installation process that perhaps require further clarification.

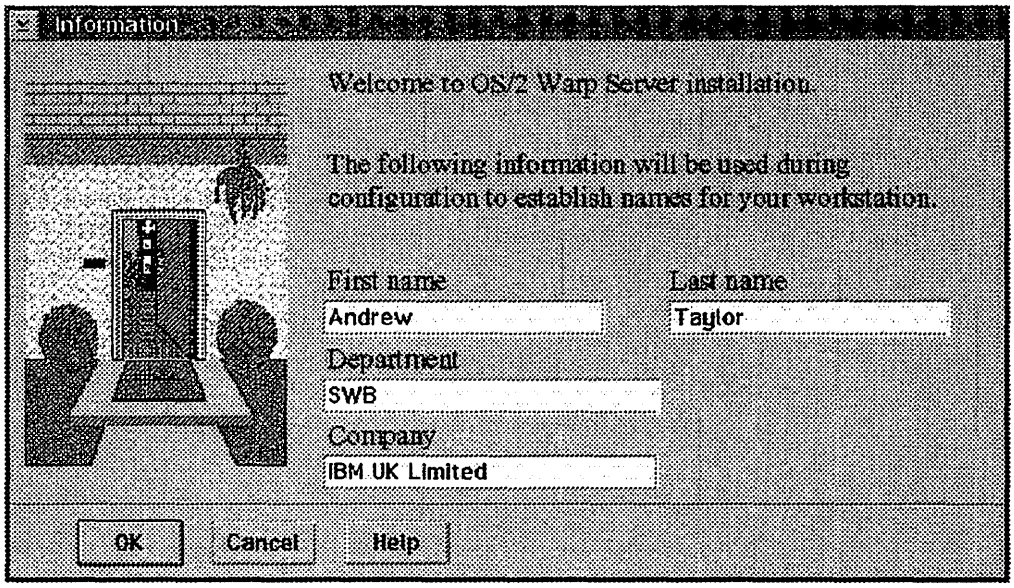


Figure 3. Welcome to OS/2 Warp Server Installation

One of the first screens that you are presented with is shown in Figure 3. Information that you provide here will be used, particularly by File and Print Sharing Services, to automatically generate the default user ID and server name, both from `Last name` and domain name, based on `Department`.

Note: You are obviously provided with options to change the server and domain name. What is new to OS/2 Warp Server is the option to specify the user ID and password of the initial administrator. In OS/2 LAN Server you were provided with an initial administrator user ID and password of USERID and PASSWORD respectively which obviously had security implications if you forgot to delete this ID or change the password after creating another administrator ID.

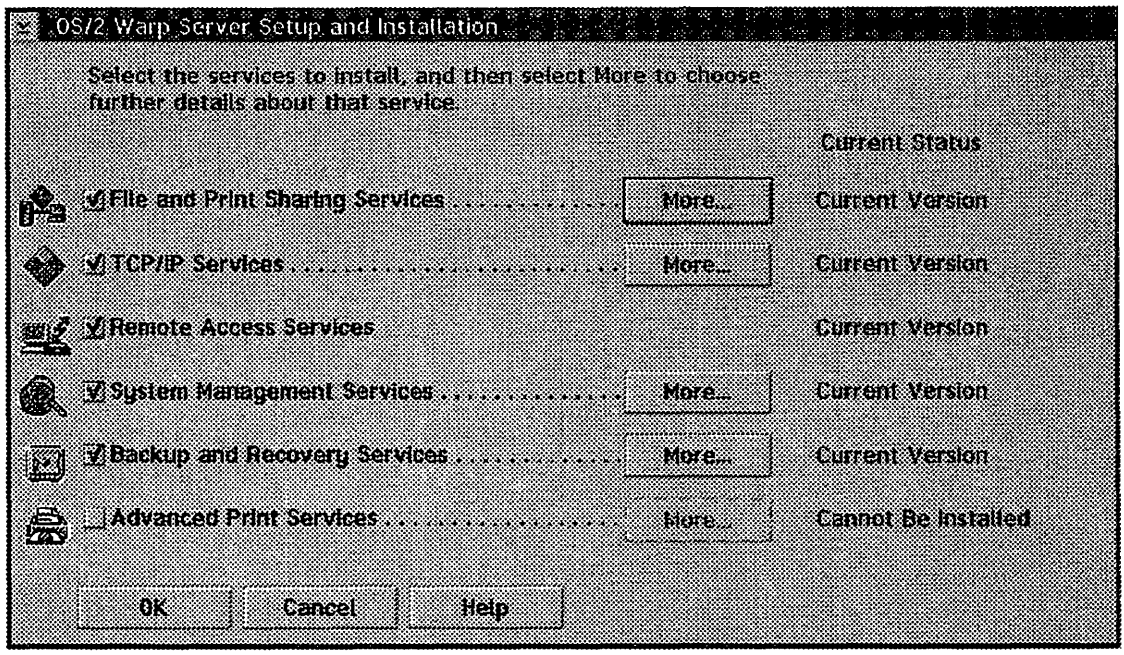


Figure 4. OS/2 Warp Server Component Installation

Selecting **More...** provides you with the option to select the specific File and Print Sharing Services features that you would like to install.

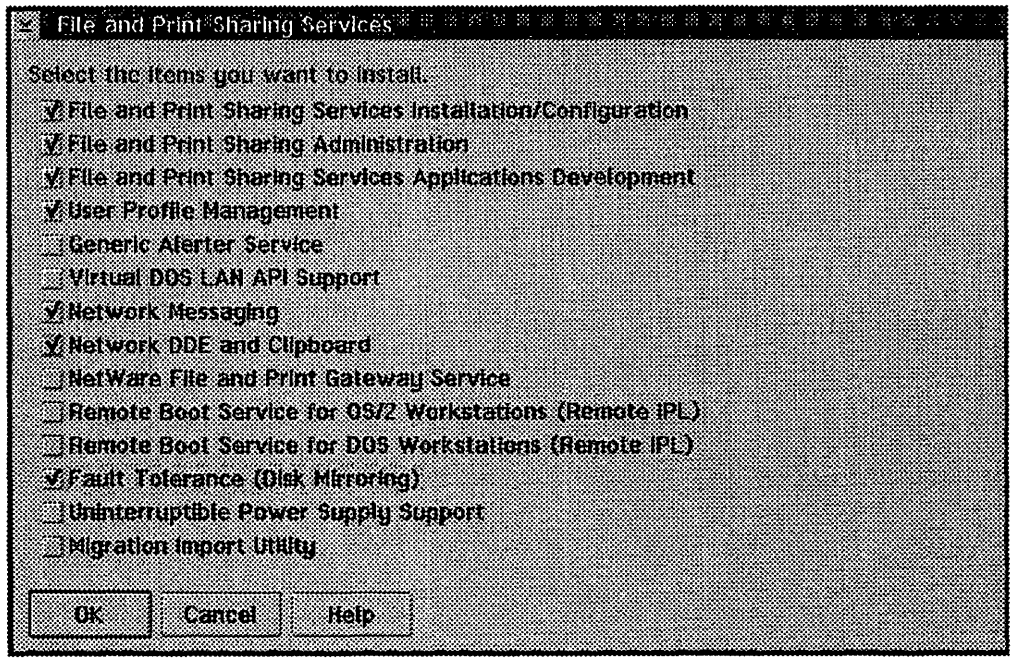

File and Print Sharing Services
Select the items you want to install.
File and Print Sharing Services Installation/Configuration
File and Print Sharing Administration
File and Print Sharing Services Applications Development
User Profile Management
Generic Alerter Service
Virtual DOS LAN API Support
Network Messaging
Network DDE and Clipboard
NetWare File and Print Gateway Service
Remote Boot Service for OS/2 Workstations (Remote IPL)
Remote Boot Service for DOS Workstations (Remote IPL)
Fault Tolerance (Disk Mirroring)
Uninterruptible Power Supply Support
Migration Import Utility
OK
Cancel
Help

Figure 5. File and Print Sharing Services Feature Installation

Each feature of File and Print Sharing Services is well documented in the online OS/2 Warp Server documentation and in OS/2 LAN Server publications so we will not discuss them in detail.

Installation Considerations

If you are using nonstandard hardware such as RAID technology or non-IBM CD-ROM drives, you need to copy necessary files to the second diskette and make necessary changes in the CONFIG.SYS file. Failure to do so might result in not being able to see devices when starting your workstation from boot diskettes.

Enabling RAID Support

1. For server machines based on RAID technology, be sure to have the latest IBMRAID.ADD driver.
   a. Internet users may retrieve that file from the IBM Personal Computer Servers homepage. Point your WEB browser to the following URL:

      `http://www.pc.ibm.com/server`

      At the end of that page there is a RAID support item in the Files section from where you can get the latest IBMRAID.ADD file.

   b. Alternatively, instead of IBMRAID.ADD, you may use the DAC960.ADD file which comes with OS/2 Warp Server. This files resides on the CD-ROM's \WARPSRV\IBMRAID subdirectory and is an updated replacement for IBMRAID.ADD.
2. Append the following line and make this line the first statement in the CONFIG.SYS file of the second boot diskette:

   `BASEDEV=IBMRAID.ADD`

   Note: If you chose DAC960.ADD as your RAID driver, you would insert the line `BASEDEV=DAC960.ADD` instead.

After OS/2 Warp Server installation, the RAID driver resides in the root directory. You may want to move that file to the \OS2\BOOT directory.

2.4 Configuration

The configuration process of the File and Print Sharing Services component of OS/2 Warp Server should be familiar to you if you have previously installed OS/2 LAN Server. The panels follow the look and feel of the OS/2 Warp Server integrated installation program, the flow and nature of the questions are consistent with the OS/2 LAN Server installation process as Figure 7 on page 14 illustrates.

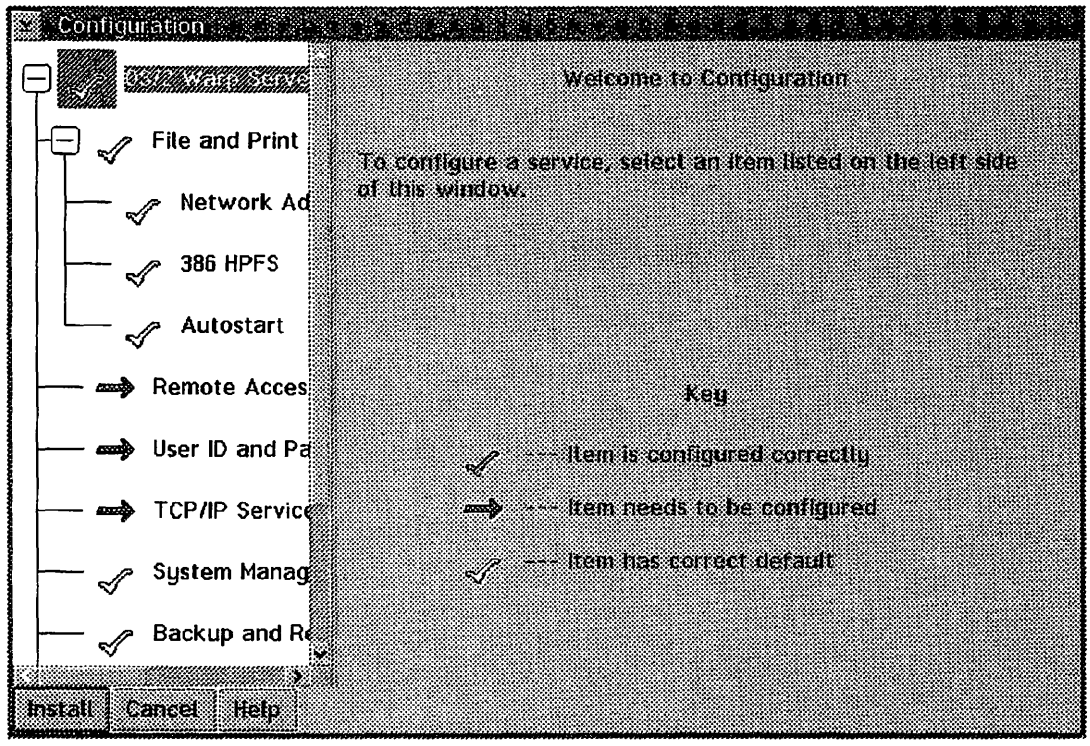


Figure 6. OS/2 Warp Server Component Configuration

The inexperienced and experienced network administrator are both catered to by providing easy and advanced installation paths. The advanced path is illustrated in Figure 7.

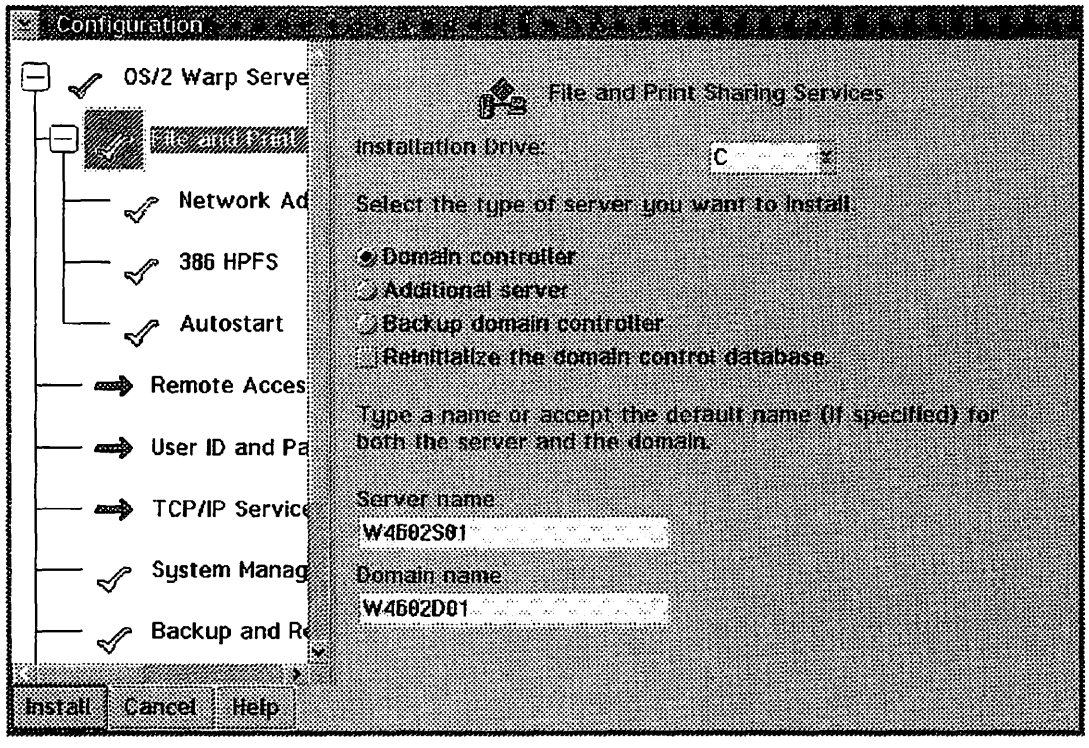


Figure 7. File and Print Sharing Services Feature Configuration

2.5 OS/2 Warp Server Tuning Assistant

OS/2 Warp Server and OS/2 Warp Server Entry are tuned to support 100 and 32 concurrently connected users respectively. Once you have installed and configured OS/2 Warp Server File and Print Sharing Services you should fine tune OS/2 Warp Server to satisfy your specific installation requirements.

The Tuning Assistant provides automatic tuning and configuration of your OS/2 Warp Server workstation.

OS/2 Warp Server does not dynamically retune itself as you add more requesters. If you have a growing OS/2 Warp Server environment then you need to run this utility at regular intervals to verify that your OS/2 Warp Server configuration can support the number of users connecting to resources and provide optimum performance.

Attention

Please note that the majority of problems you may encounter with OS/2 LAN Server and OS/2 Warp Server are likely to be capacity related.

When you start the Tuning Assistant by selecting the appropriate object from the LAN Services Folder, as shown in Figure 2 on page 7, and click on **OK**, you are presented with the screen as shown in Figure 8.

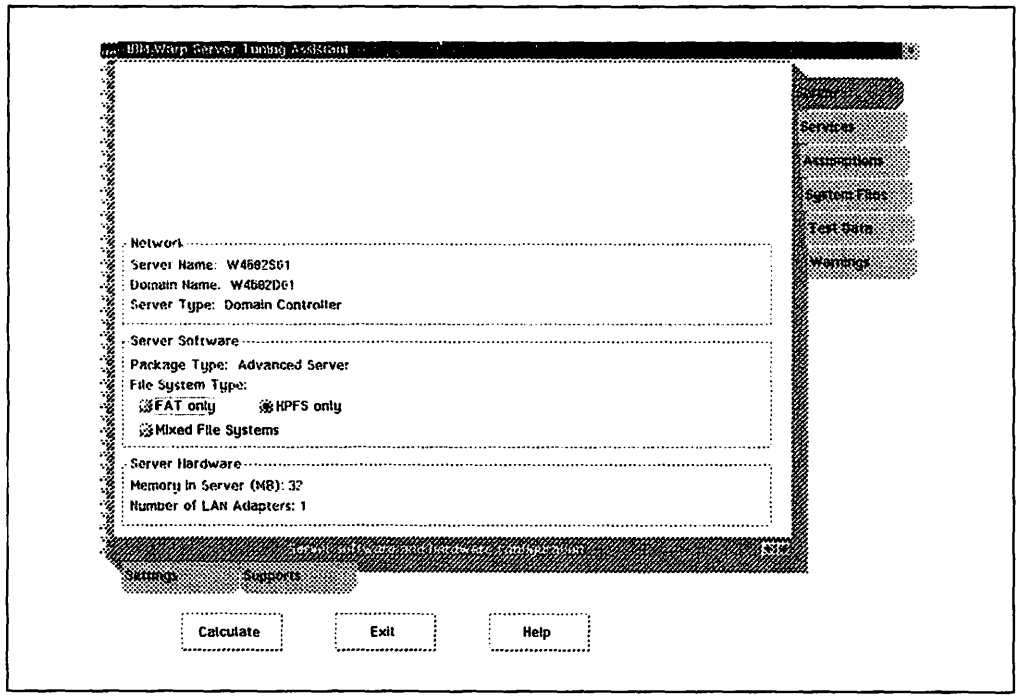


Figure 8. Server Hardware and Software Configuration Summary

Note: The OS/2 Warp Server Tuning Assistant is designed to tune server workstations and will try to detect your server software configuration. Therefore, if you attempt to execute WSTUNE.EXE at a requester you will receive the error as shown in Figure 9 on page 16. It is, however, possible to run WSTUNE.EXE on a requester by providing a sample configuration to be processed. You can

find details on how to do this in "Running the Tuning Assistant on a Requester" on page 18.

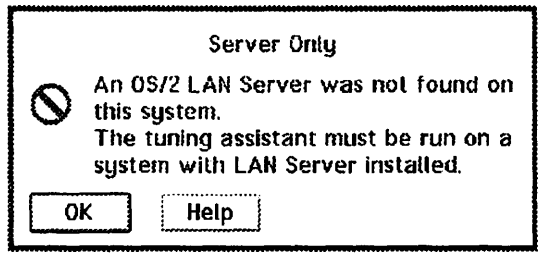

Server Only
An OS/2 LAN Server was not found on this system.
The tuning assistant must be run on a system with LAN Server installed.
OK
Help

Figure 9. Running the Tuning Assistant on a Requester

The Tuning Assistant automatically detects key network, software and hardware configuration information and, based on the information that you provide, will generate warnings if you exceed the server workstation's capacity to support your configuration.

As you can see in Figure 10, the Tuning Assistant recommended that additional server RAM and network adapters be added.

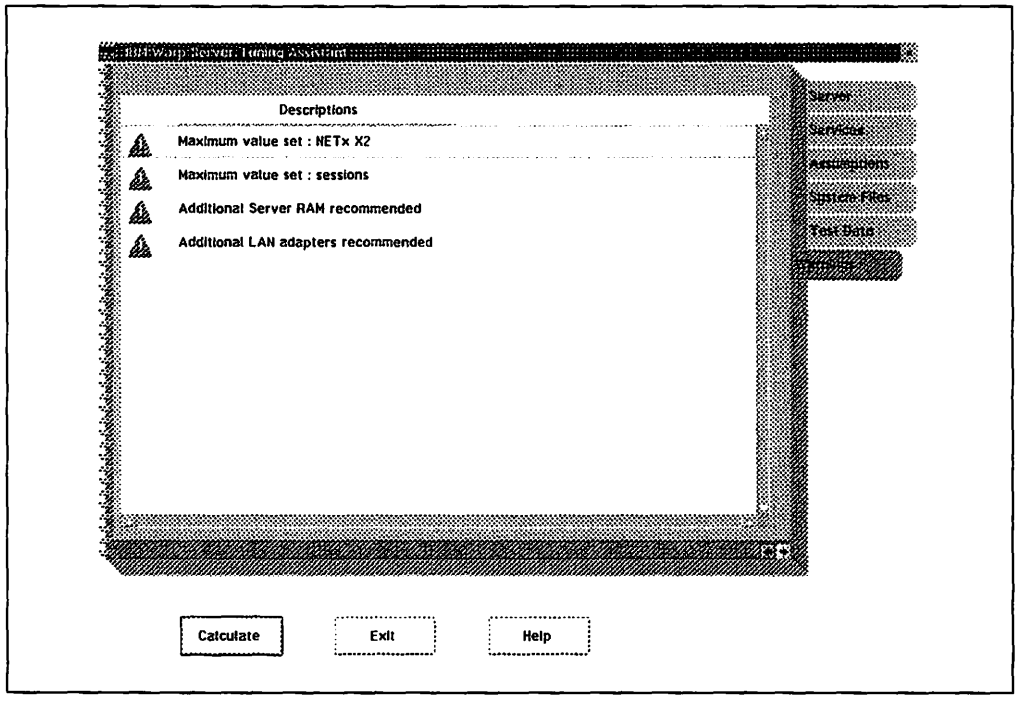


Figure 10. Configuration Warnings/Recommendations Screen

In it's present form, the Tuning Assistant was first introduced in OS/2 LAN Server 4.0. The OS/2 Warp Server Tuning Assistant is a natural development of this utility and includes variables for other key components that may affect OS/2 Warp Server performance or capacity.

Figure 11 on page 17 shows an example of how the LAN Server Tuning Assistant has been enhanced to include the requirements of Remote Access Services and other key OS/2 Warp Server components in the tuning calculation.

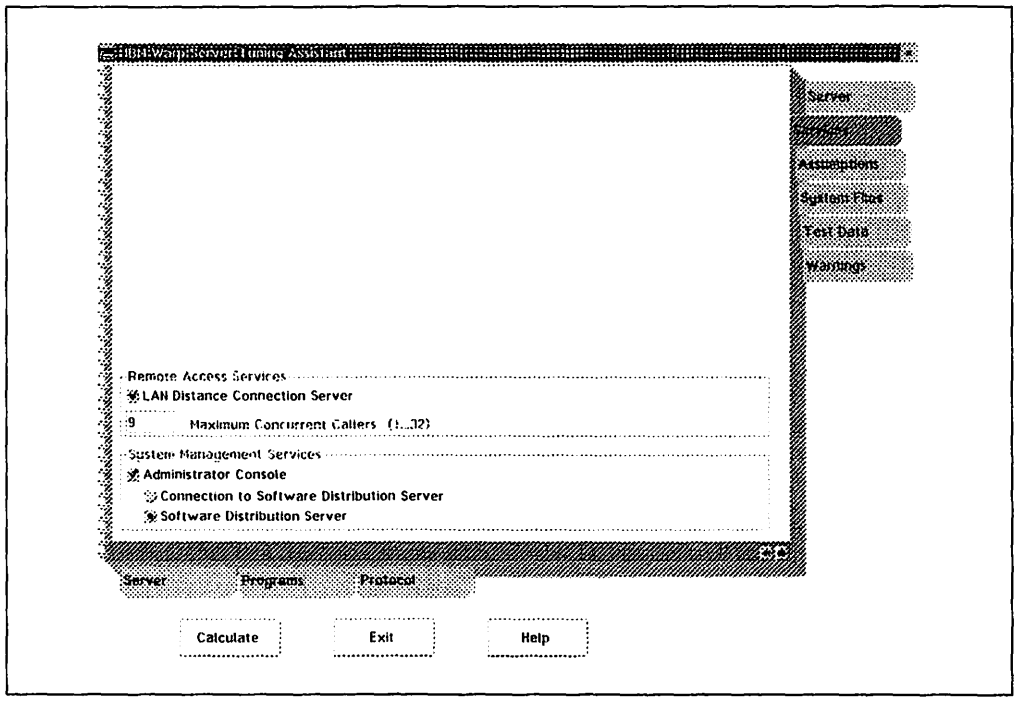


Figure 11. OS/2 Warp Server Component Requirements (Server)

Once you have completed all the panels by typing in your specific environment variables you then select **Calculate**. If any warnings are generated at this point you will be informed via the pop up window as shown in Figure 12.

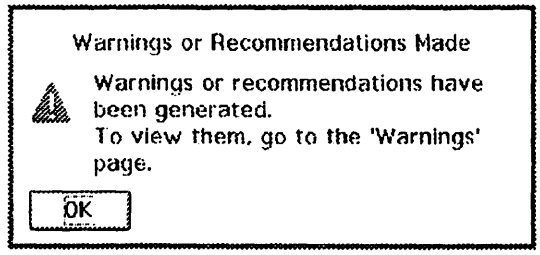

Warnings or Recommendations Made
Warnings or recommendations have been generated.
To view them, go to the 'Warnings' page.
OK

Figure 12. Warnings or Recommendations Made

The Updated Files list now includes the Remote Access Services WCLLOCAL.INI configuration file (when Remote Access Services is configured) as shown in Figure 13 on page 18.

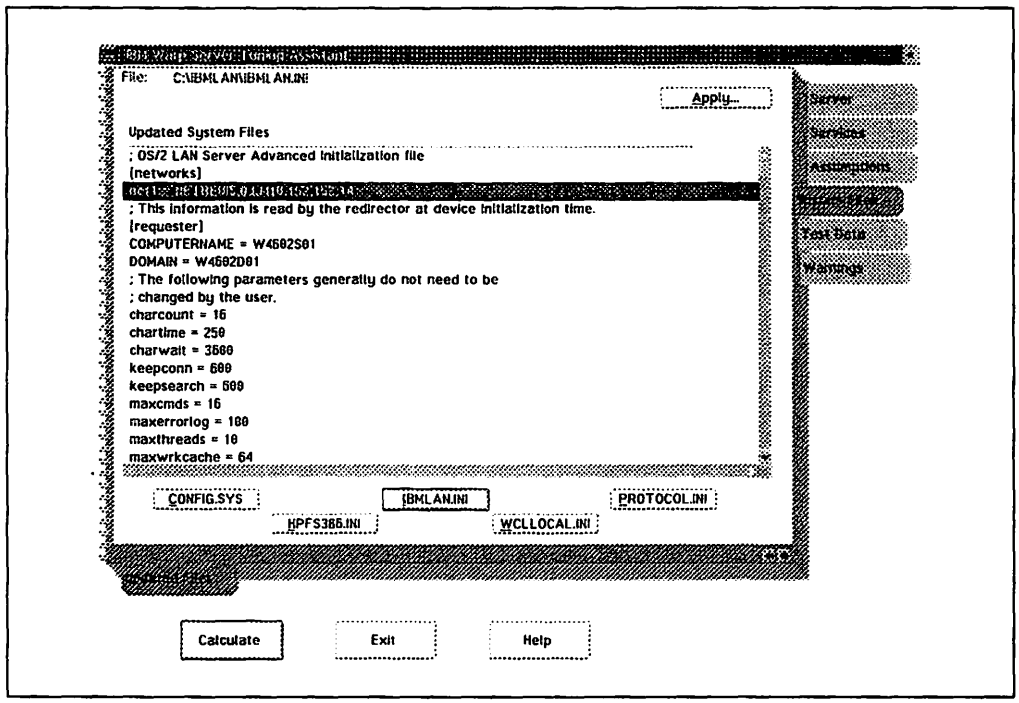


Figure 13. Updated Files Screen

If you are happy with the suggested modifications to each file (which are highlighted) then you may put them into effect the next time the system is started by simply selecting **Apply**.

Note: Backup copies of the existing configuration files will be stored in \IBMLAN\BACKUP.

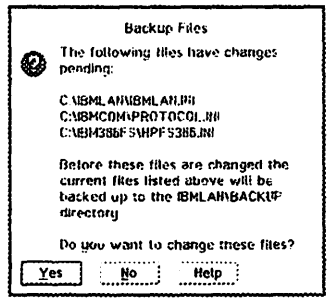


Figure 14. Backup Files Confirmation Window

Running the Tuning Assistant on a Requester

As mentioned earlier in this chapter, the Tuning Assistant is designed to tune server workstations and therefore is not installed on requesters. If you attempt to run WSTUNE.EXE on a requester then you will receive an error.

If you wish to build configuration files for servers on your requester then you may do so by first copying WSTUNE.EXE from a server workstation and running it in an OS/2 windowed or full screen session, supplying a number of parameters from the following list:

- [/D:] enables you to specify the name of the domain that the server workstation will belong to.

- [/S:] enables you to specify the name of the server workstation that you wish to generate the configuration files for.
- [/T:] enables you to specify the role of the server. You may select DC or AS for domain controller or additional server respectively.
- [/P:] allows you to specify the package type (ENTRY or ADVANCED).
- [/M:] specifies how much memory is installed in the server (MB).
- [/A:] specifies the number of network adapters you want the configuration file to support (to a maximum of 4).
- [/U] specifies that you want to use copies of configuration files (CONFIG.SYS, IBMLAN.INI, PROTOCOL.INI, HPFS386.INI, WCLLOCAL.INI, WSCONFIG.CFG) stored in the current subdirectory to generate the tuned configuration files.

Notes:

1. When specifying package type via the /P parameter, select ENTRY for an OS/2 Warp Server Entry server and ADVANCED for an OS/2 Warp Server Advanced server.
2. If you apply calculated changes to files in the current subdirectory no backups are created.
3. /T is always required along with /U if no server is installed.

For example, if you wish to build and verify a specific configuration for an OS/2 Warp Server workstation you would enter:

```
WSTUNE /D:W4602D01 /S:W4602S01 /T:DC /P:ADVANCED /M:64 /N:4 /U
```

Figure 15. Running WSTUNE.EXE on a Requester

Note: These parameters may also be used with the OS/2 LAN Server 4.0 Tuning Assistant (LSTUNE.EXE).

2.6 Sharing Resources with the Administration GUI

In this section we will look at how you define shared resources from the Administration Graphical User Interface (GUI). This interface, as shown in Figure 16 on page 20, may be accessed from the LAN Services folder or from the Network folder on the OS/2 Warp Server Desktop and enables you to do the following:

- Manage OS/2 Warp Server users and groups, including the definition of how shared resources appear to them and which network applications appear in the Network Applications folder on their Desktop when they logon. These definitions are referred to as *logon assignments*.
- Define resources that you want to share, known as *aliases*.
- Specify what permissions users have to access each shared resource.
- Define and provide access to applications that are stored on server workstations but may be executed from requesters.
- Manage server workstations on the network.
- Connect to resources that you want to use and manage your own network applications.

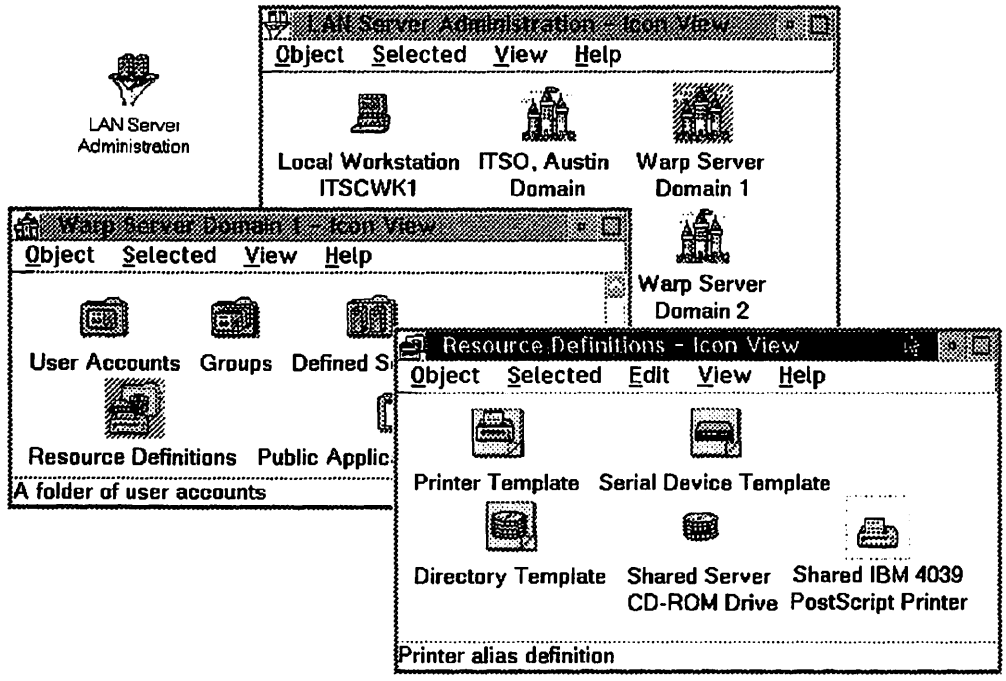


Figure 16. OS/2 Warp Server Administration Graphical User Interface

OS/2 Warp Server shared resources are defined in the Resource Definitions folder (the active window in Figure 16).

There are three templates which you use to create shared directories, printers and serial device. You define the server workstation resources by simply selecting the template that matches the type of shared resource that you want to share with mouse button 2 and drag and drop the template to an area within the folder. In the next two sections we will look at how you share files and printers from the OS/2 Warp Server Administration GUI.

Sharing Files with the Administration GUI

OS/2 Warp Server provides access to shared files by enabling you to create shared directories in which the files are stored. To share a directory you must be logged on as an administrator or a user with a privilege level to manage shared resources.

To share a directory with users:

1. Start the Administration GUI.
2. Select the domain that you wish to manage.
3. Open the Resource Definitions Folder.
4. Select the **Directory Template** icon, and, while holding down mouse button 2, drag the icon to an open area in the Resource Definitions folder and release the button. The **Directory Alias - Create** notebook is displayed, as shown in Figure 17 on page 21.

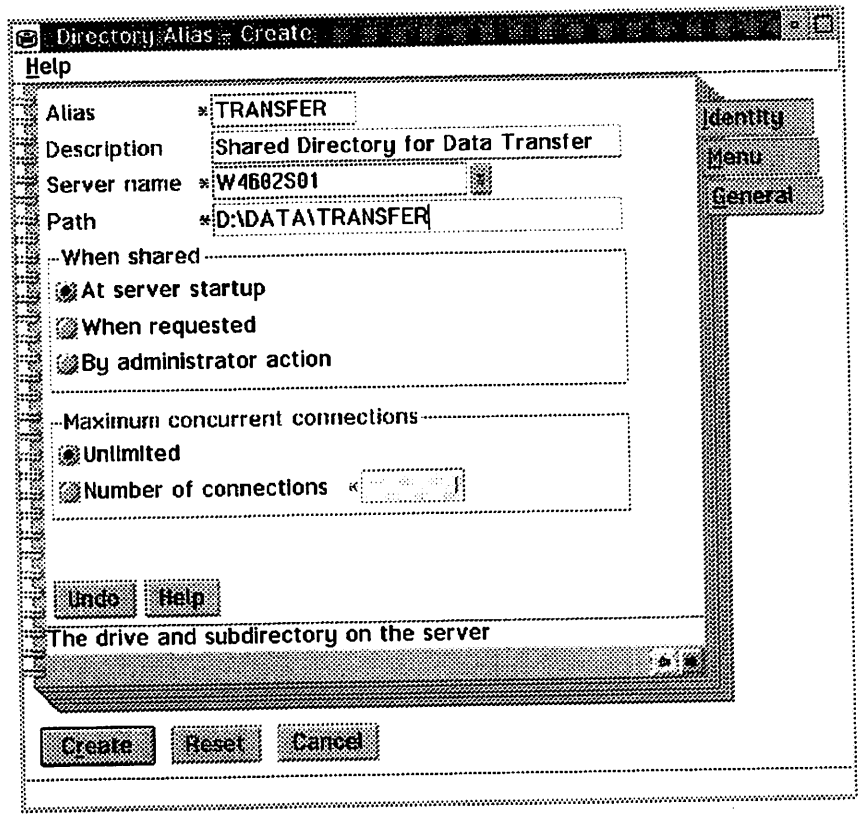


Figure 17. Directory Alias - Create notebook

Note: A directory does not need to exist before it can be shared. OS/2 Warp Server will automatically create the directory as part of the resource definition process.

5. Complete the notebook fields then select **Create**. The **Access Control Profile Does Not Exist** window, shown in Figure 18, notifies you that you need to define user's access to this resource.

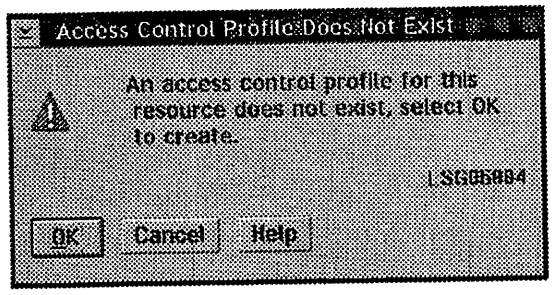

Access Control Profile Does Not Exist
An access control profile for this resource does not exist, select OK to create.
SGDH004
OK
Cancel
Help

Figure 18. Access Control Profile Does Not Exist Window

Note: To create a shared directory definition without defining an access control profile, select **Cancel**.

6. Select **OK** to display the Access Control Profile notebook, select the **Permissions** page then **Add**.
7. You then select the users or groups that you want to have access to this alias and select the permissions that you want them to have, as shown in Figure 19 on page 22, and click on **OK**.

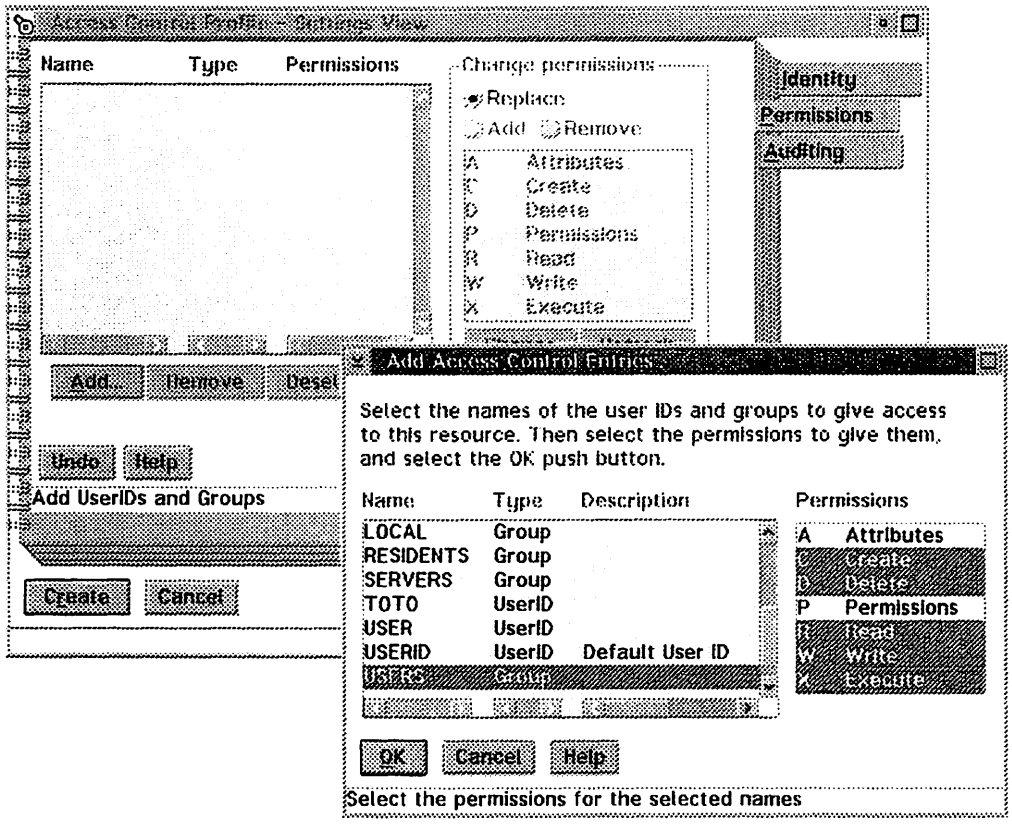


Figure 19. Defining an Access Control Profile for a Shared Directory

8. Select **Create** and click on **OK** to propagate the access control profile so that the access permissions that we have defined take effect for files contained in subdirectories of the shared directory.

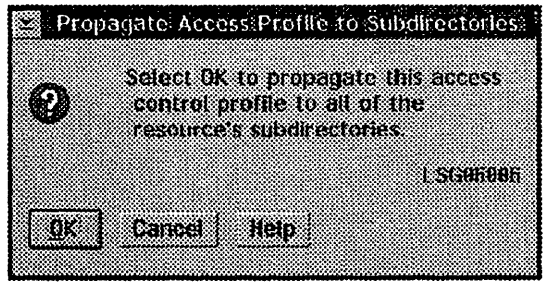

Propagate Access Profile to Subdirectories
Select OK to propagate this access control profile to all of the resource's subdirectories.
OK
Cancel
Help

Figure 20. Propagate Access Control Profile to Subdirectories Window

Once you complete the above procedure the directory is shared and available to be accessed. There is nothing else that you need to do other than providing users or groups with logon assignments so they may connect to and use the shared directory.

Note: If you selected **Cancel** at the point where you were asked whether you you wanted to create an access control profile for the resource (Figure 18 on page 21) you could subsequently manage access to the resource and propagate the access control profile by simply selecting the resource object with mouse button 2 and then clicking on the appropriate context menu item as shown in Figure 23 on page 25. This is a good illustration of how OS/2 Warp Server integrates seamlessly with the Work Place Shell.

Sharing Printers with the Administration GUI

As is the case with creating shared directories, to define a shared printer resource you must be logged on as an administrator. In the following example you will notice that with OS/2 Warp Server you don't share a physical printer port you share an OS/2 print queue.

To share a printer with users:

1. Start the Administration GUI.
2. Select the domain that you wish to manage.
3. Open the Resource Definitions Folder.
4. Select the **Printer Template** icon, and, while holding down mouse button 2, drag the icon to an open area in the Resource Definitions folder and release the button. The **Printer Alias - Create** notebook is displayed, as shown in Figure 21.

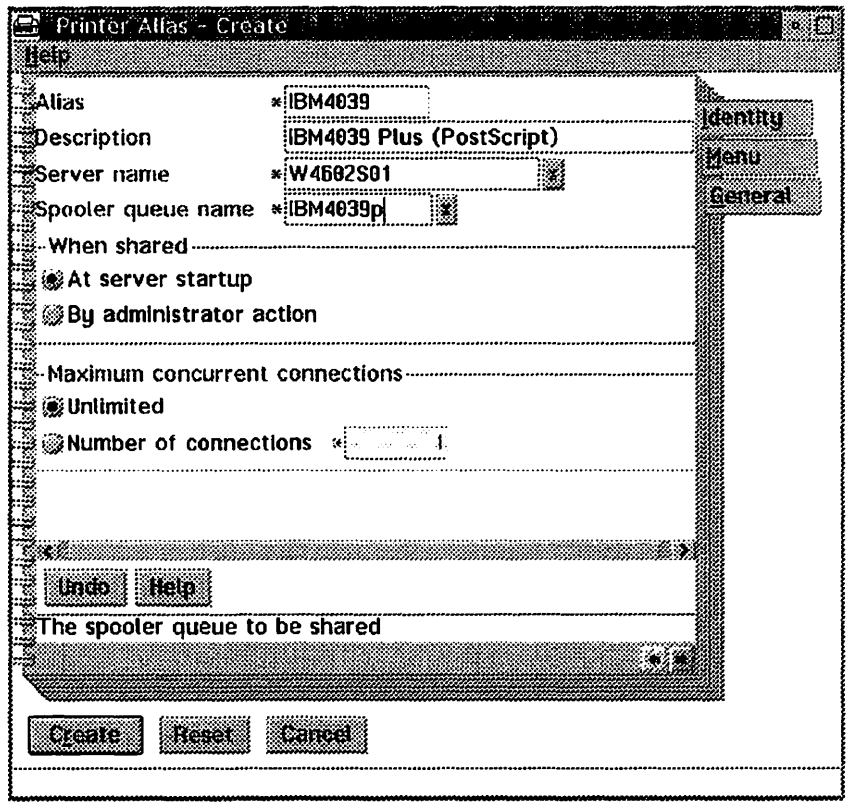


Figure 21. Printer Alias - Create notebook

5. Complete the notebook fields then select **Create**. The same **Access Control Profile Does Not Exist** window, as shown in Figure 18 on page 21, notifies you that you need to define user's access to this resource.

   Note: To create a shared printer definition without defining an access control profile, select **Cancel**.

6. Select **OK** to display the Access Control Profile notebook, select the **Permissions** page then **Add**.
7. Select the users or groups you want to have access to this alias and select the permissions that you want them to have, as shown in Figure 22 on page 24, and click on **OK**.

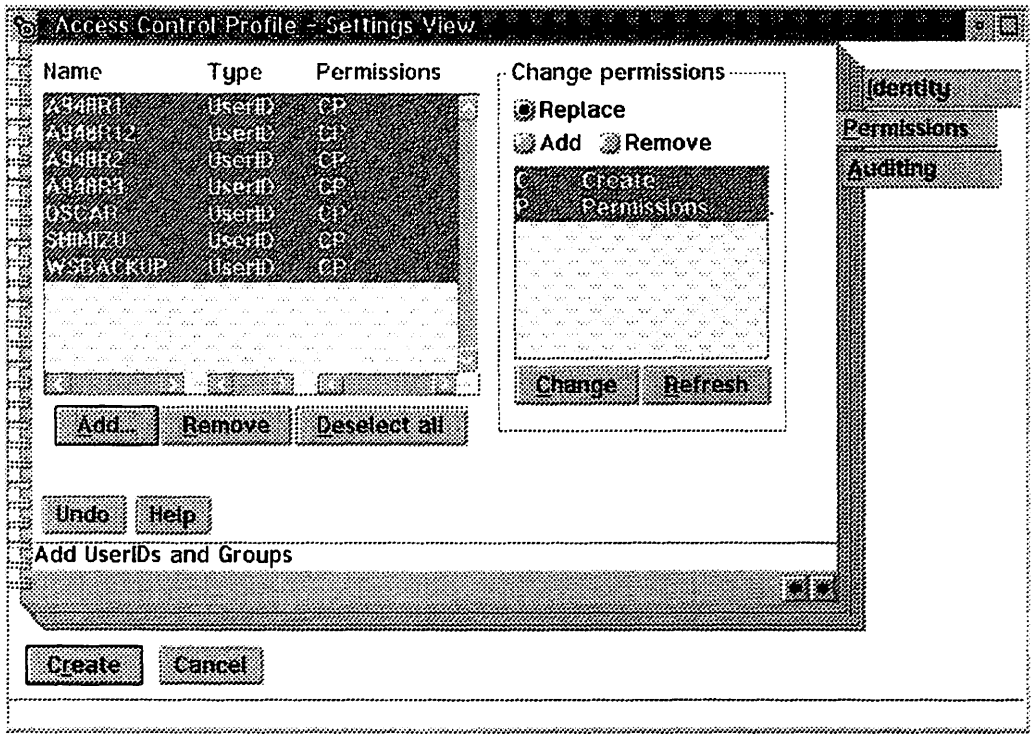


Figure 22. Defining an Access Control Profile for a Shared Printer

8. Select **Create**.

Once you complete the above procedure the printer queue is shared and available to be accessed. There is nothing else that you need to do other than providing users or groups with logon assignments so they may connect to and use the shared printer.

Note: By using the drag and drop capabilities of the Administration GUI you may provide groups of users with logon assignments by simply dragging a shared resource and dropping it on a group of users, and vice versa.

Support for Thousands of Aliases

With OS/2 Warp Server you may define thousands of shared resources, known as *aliases*, via the Administration GUI. This is a notable enhancement to the LAN Server 4.0 Administration GUI which was restricted in the total number of shared resource definitions that could be displayed due to a 64KB data limitation.

To give you an idea of what performance you can expect when administering thousands of aliases we performed some tests. To open the Resource Definitions folder on a server workstation with a 90MHz Pentium processor took 45 seconds with 2000 aliases defined, and 2½ minutes for 4100 aliases to be displayed.

2.7 Other Methods of Sharing Resources

The OS/2 Warp Server Administration GUI is just one way of sharing resources in an OS/2 Warp Server environment. In this section we will look at the other options provided for sharing resources and managing access to them.

You can also share resources and manage access to them from:

- OS/2 Warp Server Desktop
- OS/2 Command Line
- Current shares window

These additional options may be used as an alternative to the Administration GUI, although administration by the manipulation of desktop objects is dependent upon the Administration GUI being loaded.

Sharing Resources from the Desktop

As mentioned at the beginning of this chapter, the Administration GUI is integrated with the OS/2 Warp WorkPlace Shell. This means that you have access to additional menu options to start sharing, stop sharing, manage access to, and (for directory objects) manage limits.

The following examples in Figure 23 and Figure 24 on page 26 show the results of selecting an object on the desktop with mouse button 2.

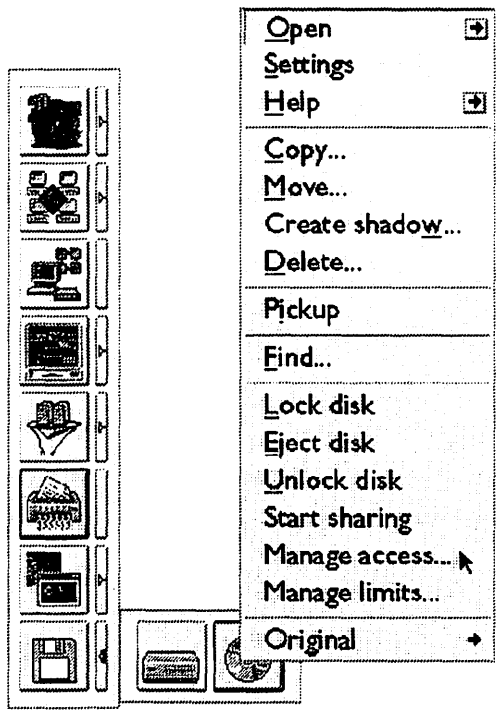


Figure 23. Network Extensions to Desktop Drive Object

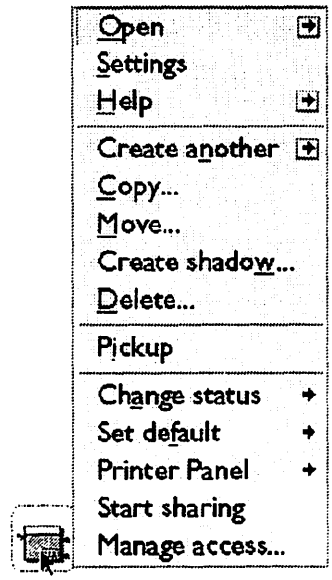


Figure 24. Network Extensions to Desktop Printer Object

Selecting any of the menu network options will present you with the appropriate notebook from the Administration GUI.

Example: Sharing a CD-ROM Drive

To share a CD-ROM drive by alias perform the following steps:

1. From the Administration GUI, create an directory alias. Complete the fields on the Identity page as follows:
   - Alias Name: `CDROMDRV`
   - Description: `Server's CD-ROM Drive`
   - Server: `W4602S01`
   - Path: `D:\.`
   - When Shared: At Server Startup
   - Maximum concurrent connections: Unlimited
2. Select **Create**.
3. Select **Cancel** at the Access Control Profile Does Not Exist window.

   The directory alias will be created for you now.
4. In the Drives folder which resides in the OS/2 System folder, display the CD-ROM drive's object pop-up menu by using mouse button 2 as shown in Figure 23 on page 25.
5. Select **Manage access ...** which will display the Identity page of the Access Control Profile notebook.
6. Select **OK** at the Access Control Profile Does Not Exist window.
7. Select the **Permissions** tab.
8. Select **Add ...**

   The Add Access Control Entries window is displayed.

9. Select the user IDs or group IDs you want to allow access to the CD-ROM drive. Select the permissions you want to grant to the users and groups you selected.

   Note: If you generally want to allow access to the CD-ROM drive you might select the group called Users and grant Read and Execute (RX) permissions.

10. Select **OK**.

11. Select **Create**.

    The access control profile for the CD-ROM drive is created.

Sharing Resources from the Command Line

Every task that you can perform from the GUI may also be performed from the OS/2 command line. This is very useful as it enables repetitive tasks, such as the creation of many users and their logon assignments, to be automated via OS/2 command files or REXX scripts.

For example, the following series of commands would produce the same results as the scenario we looked at in "Sharing Files with the Administration GUI" on page 20.

```
NET ALIAS TRANSFER \\W4602S01 D:\DATA\TRANSFER /DO:W4602D01 /W:STARTUP /R:"Shared Directory" /UN
NET ACCESS TRANSFER /GRANT USERS:RWCDX
NET ACCESS TRANSFER /APPLY
```

Figure 25. Commands to Share a Directory Resource from the Command Line

Note: These commands will only be accepted if you are logged on as an administrator, or a user with special privileges to manage server resources.

It is possible to remotely manage the server from your DOS or Windows 95 workstation by using the `NET ADMIN` command. To perform remote administration you would prefix the command with `NET ADMIN \\servername /C`.

You will find the complete list of `NET` commands and associated parameters by typing `NET` (or `NET HELP NET command` for specific command syntax) at the command line or in the OS/2 Warp Server *Commands and Utilities* online publication.

Sharing Resources from the Current Shares Window

An administrator may query the resources that are currently being shared via the relevant **Current shares** window. In addition, as is shown in Figure 26 on page 28, you also have options to share another, change share, stop share, manage access and (for directory resources) manage limits.

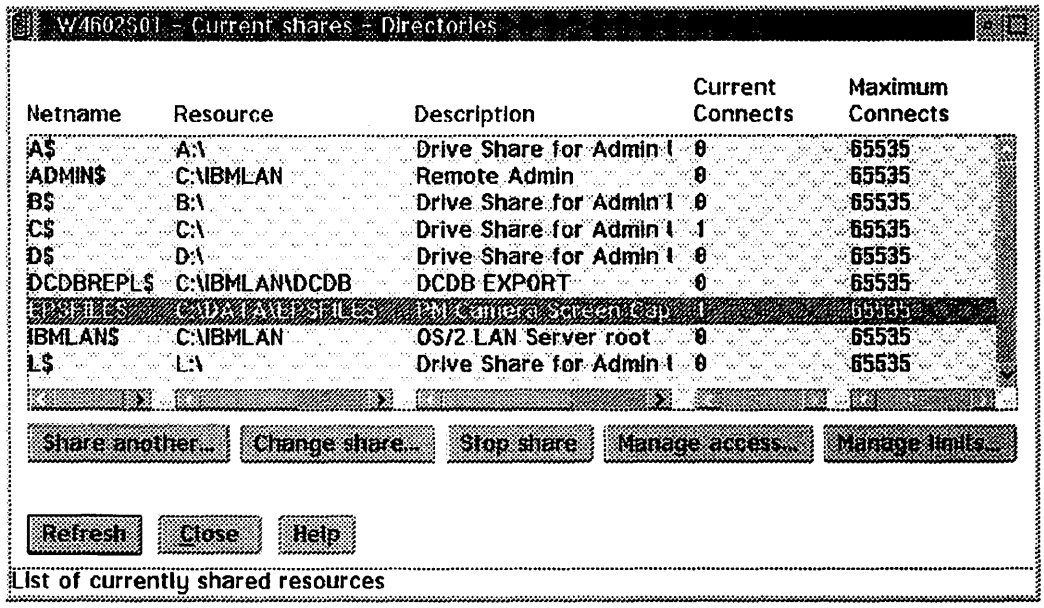

W4602501 - Current shares - Directories
Netname
Resource
Description
Current Connects
Maximum Connects
A$ A:\ Drive Share for Admin I 0 65535
ADMIN$ C:\IBMLAN Remote Admin 0 65535
B$ B:\ Drive Share for Admin I 0 65535
C$ C:\ Drive Share for Admin I 1 65535
D$ D:\ Drive Share for Admin I 0 65535
DCDBREPL$ C:\IBMLAN\DCDB DCDB EXPORT 0 65535
IBMLAN$ C:\IBMLAN OS/2 LAN Server root 0 65535
L$ L:\ Drive Share for Admin I 0 65535
Share another...
Change share...
Stop share
Manage access...
Manage limits...
Refresh
Close
Help
List of currently shared resources

Figure 26. Sharing Resources from the Current Shares - Directories Window

2.8 Preparing the Server for Client Installation

Once you have defined the resources that you want to share you need to prepare the server so that you can install clients from disk images stored on the OS/2 Warp Server CD-ROM or server's fixed disk.

Which client installation method is best for you?

If you are installing less than five clients at a time then installing from the server's CD-ROM provides a quick and easy installation method.

If you are installing more than five clients then installing from source files on the server's hard disk means that the server's CD-ROM drive is not unavailable for use for extended periods of time.

If the clients have a CD-ROM attached and/or OS/2 installed, you do *not* need to set up the server.

Make sure that you have two blank 3.5-inch diskettes ready. The OS/2 Warp Server client installation process will use these to create remote installation diskettes.

To set up the server to install OS/2 Warp Server clients across the LAN:

1. Open an OS/2 command prompt and type:

   ```
   d:
   cd warpsrv\os2clnt
   wssetup
   ```

   Where `d:` is the hard disk where OS/2 Warp Server is installed.

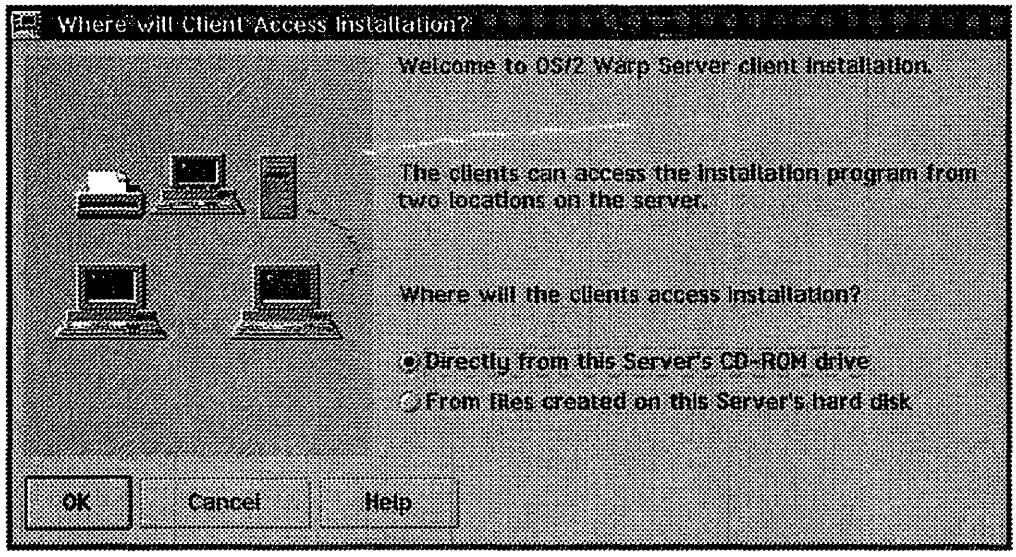

Where will Client Access Installation?
Welcome to OS/2 Warp Server client installation.
The clients can access the installation program from two locations on the server.
Where will the clients access installation?
Directly from this Server's CD-ROM drive
From files created on this Server's hard disk
OK
Cancel
Help

Figure 27. Where will Clients Access Installation? Window

2. In the Where will Clients Access Installation window, shown in Figure 27, specify whether the clients will install directly from the server workstation's CD-ROM drive or from files created on the server workstation's hard drive.

   Have the two diskettes, created as part of the server preparation for client installation, labelled *Remote Installation Diskette* and *Remote Installation Diskette - OS/2 Diskette 1*, available.

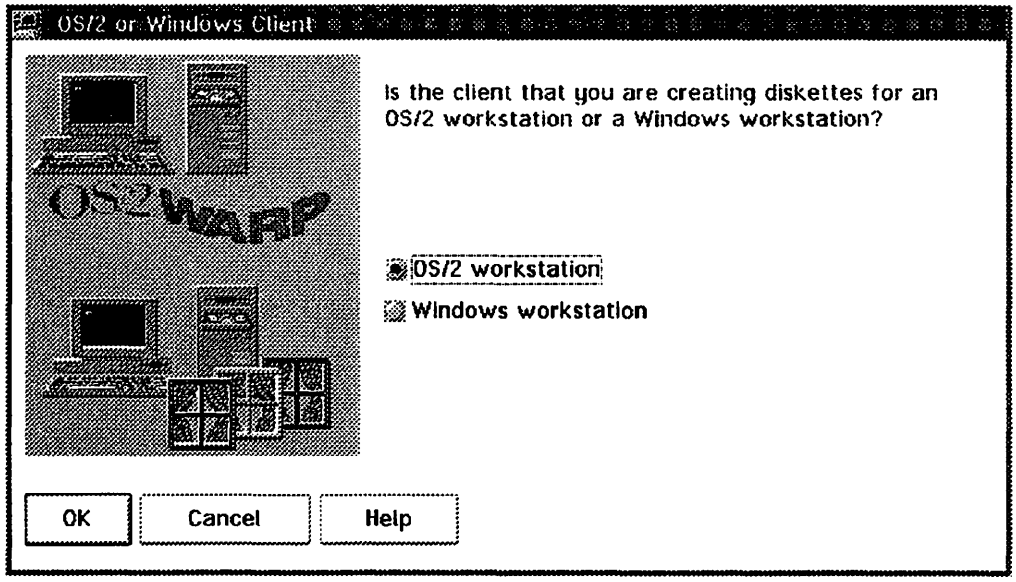


Figure 28. File and Print Client Selection

3. After you have specified where the OS/2 Warp Server source code is located you then specify whether to install an OS/2 or Windows client, as shown in Figure 28.

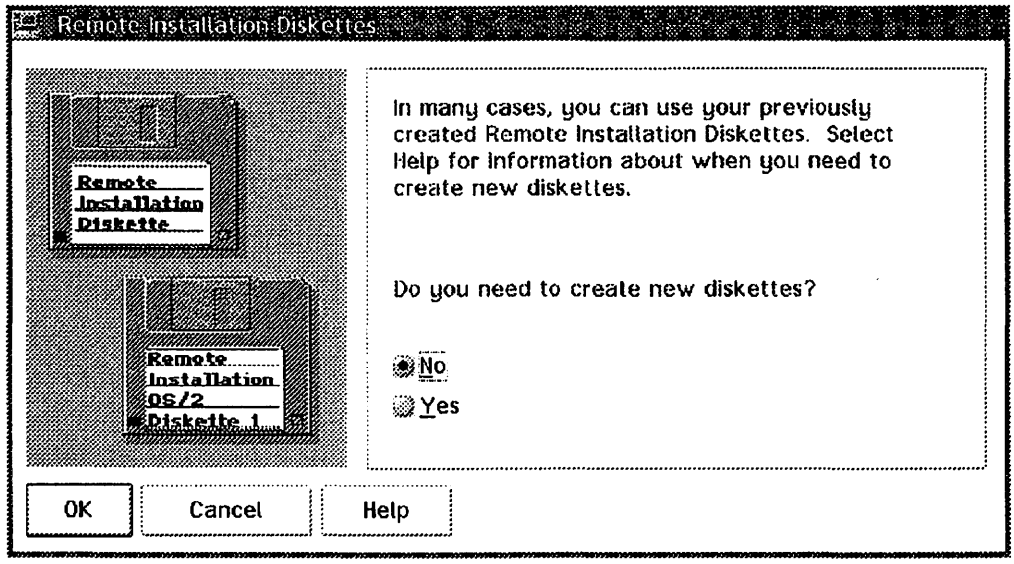

Remote Installation Diskettes
Remote Installation Diskette
Remote Installation OS/2 Diskette 1
In many cases, you can use your previously created Remote Installation Diskettes. Select Help for information about when you need to create new diskettes.
Do you need to create new diskettes?
No
Yes
OK
Cancel
Help

Figure 29. Remote Installation Diskette Creation

4. If you have previously created the remote installation diskettes and simply wish to install another client then you can skip the diskette creation step. If you need to create a new a new Remote Installation Diskette (OS/2 Diskette 1) for a client with a different network adapter then you can select **Yes** to create new diskettes and select **Skip** when prompted to create the first Remote Installation Diskette.

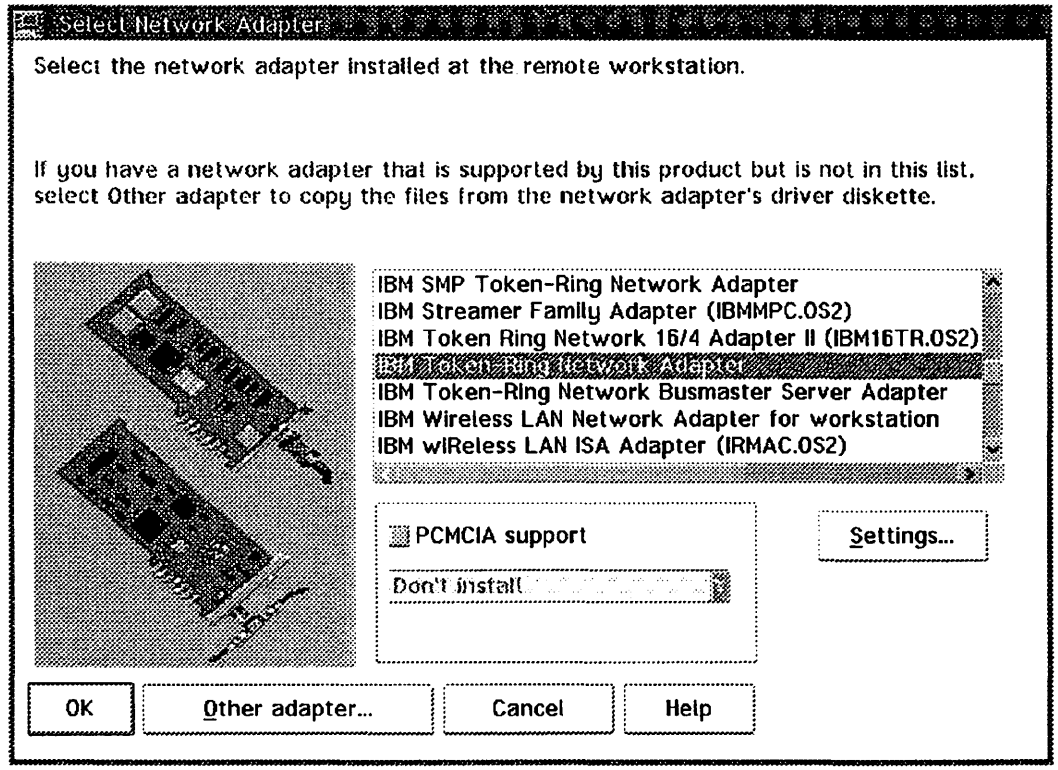

Select Network Adapter
Select the network adapter installed at the remote workstation.
If you have a network adapter that is supported by this product but is not in this list, select Other adapter to copy the files from the network adapter's driver diskette.
IBM SMP Token-Ring Network Adapter
IBM Streamer Family Adapter (IBMMPC.OS2)
IBM Token Ring Network 16/4 Adapter II (IBM16TR.OS2)
IBM Token-Ring Network Busmaster Server Adapter
IBM Wireless LAN Network Adapter for workstation
IBM wIReless LAN ISA Adapter (IRMAC.OS2)
PCMCIA support
Don't install
Settings...
OK
Other adapter...
Cancel
Help

Figure 30. File and Print Client Network Adapter Selection

5. In the window shown in Figure 30 you select the network adapter that is present in the remote client, make adjustments to any settings that are

required, and continue with the server workstation setup process described in Figure 31 on page 31.

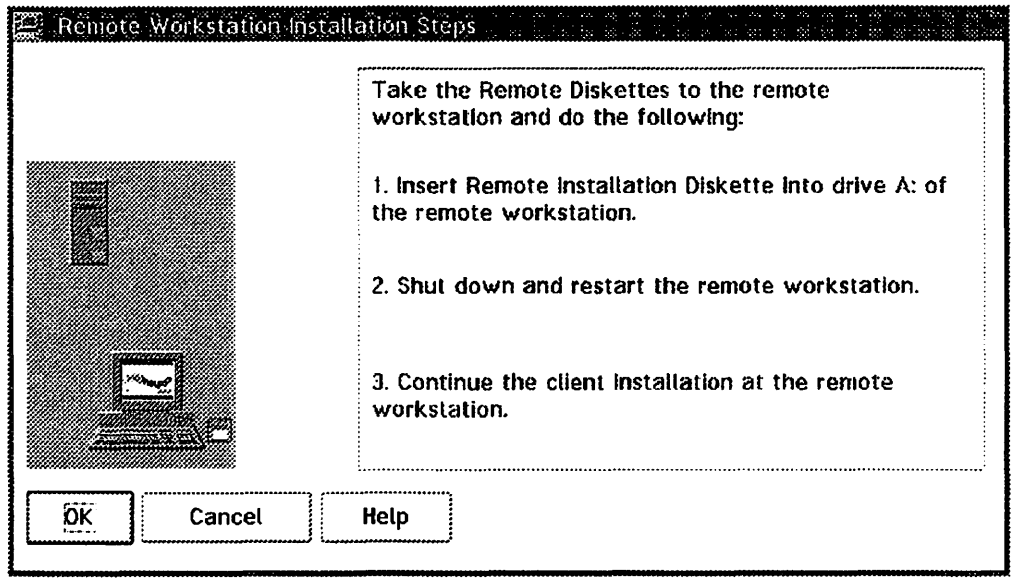

Remote Workstation Installation Steps
Take the Remote Diskettes to the remote workstation and do the following:
1. Insert Remote Installation Diskette into drive A: of the remote workstation.
2. Shut down and restart the remote workstation.
3. Continue the client installation at the remote workstation.
OK
Cancel
Help

Figure 31. Remote Installation Process

6. Once you have completed the previous steps you select **OK** and the window shown in Figure 32 will be displayed which will report on the number of OS/2 and Windows workstations attached and show whether the server is available to distribute code.

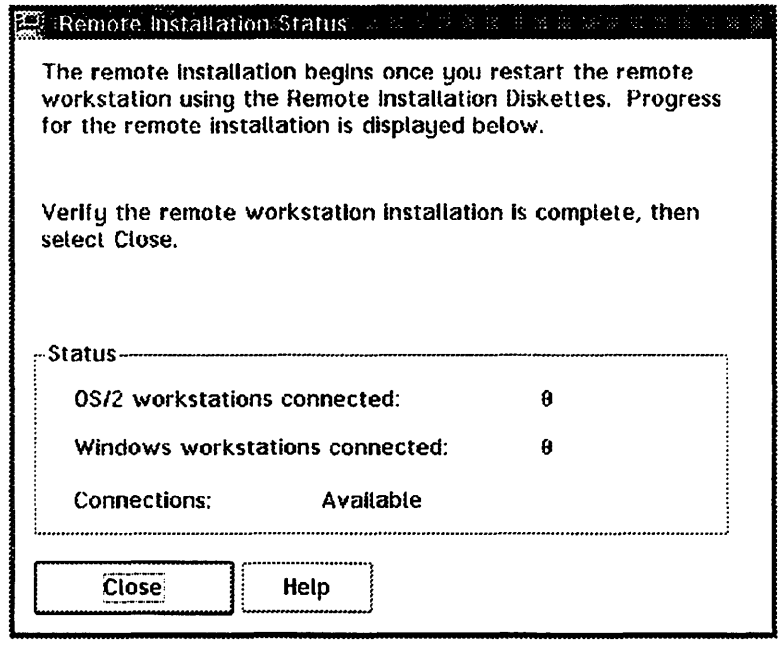

Remote Installation Status
The remote installation begins once you restart the remote workstation using the Remote Installation Diskettes. Progress for the remote installation is displayed below.
Verify the remote workstation installation is complete, then select Close.
Status
OS/2 workstations connected: 0
Windows workstations connected: 0
Connections: Available
Close
Help

Figure 32. Remote Installation Status Window

Now the server workstation is set up to allow you to remotely install the clients. Remote client installation is discussed in "Installation" on page 51.

Security Consideration

When a server workstation is running as a remote installation server it sets up SRVIFS thus giving free access to the entire drive where the images are stored. If you have confidential or private information also installed on the same drive as the images, then you will have a security risk with that confidential information.

2.9 Removing File and Print Sharing Services

If you need to remove File and Print Sharing Services from a server workstation you may do so by selecting **OS/2 LAN Services Installation/Configuration** from the IBM LAN Services folder, taking the **Tailored** installation path and selecting **Remove LAN Server from this workstation**, as shown in Figure 33.

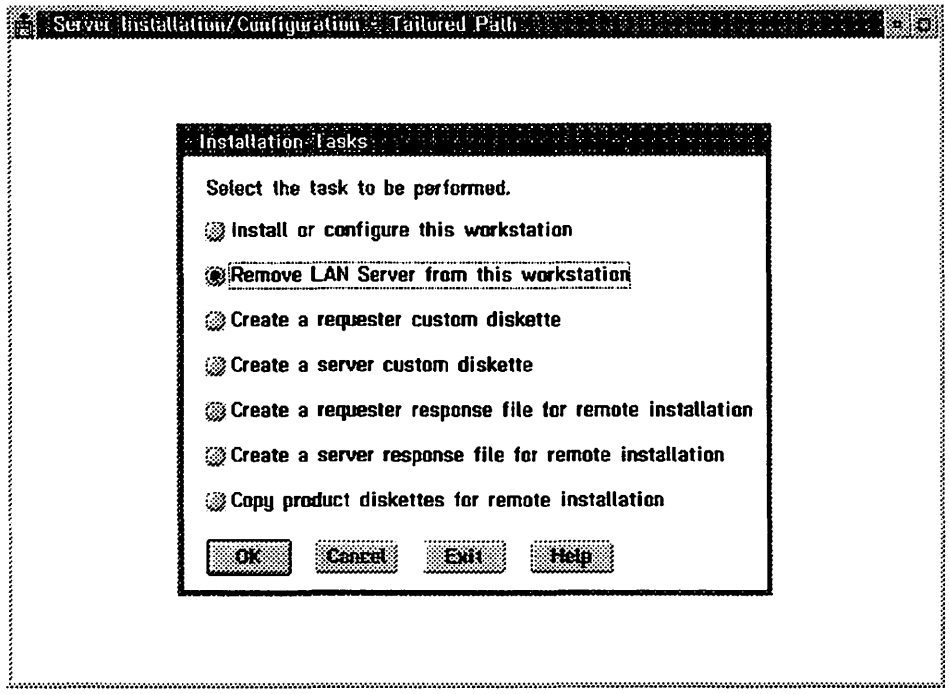

Server Installation/Configuration - Tailored Path
Installation Tasks
Select the task to be performed.
Install or configure this workstation
Remove LAN Server from this workstation
Create a requester custom diskette
Create a server custom diskette
Create a requester response file for remote installation
Create a server response file for remote installation
Copy product diskettes for remote installation
OK
Cancel
Exit
Help

Figure 33. Removing File and Print Sharing Services

2.10 OS/2 Warp Server Gateway Services

In this section we discuss the use of OS/2 Warp Server as a File and Print Gateway to other file and print subsystems. This feature is not unique to OS/2 Warp Server and can be implemented using the IBM Peer for OS/2 Version 1.0 component of OS/2 Warp Connect or previous versions of OS/2 LAN Server. Additional software may be required depending on the type of gateway you wish to implement.

It is assumed in this chapter that you have some understanding of the different file and print subsystems.

Overview and Concepts

With OS/2 LAN Server the ring 3 server can share any logical drive available to OS/2 with the exception of those redirected through OS/2 LAN Server. This means that OS/2 LAN Server can be used as a gateway between OS/2 LAN Server clients and different file and print sharing environments. The ring 3 server can also share print queues that are defined for redirected LPT ports.

This is method of sharing logical devices is also called *double redirection*.

Although this implementation has some limitations it is at times financially, or for some other reason, a viable solution. In this section we will describe the use of OS/2 Warp Server as a File and Print gateway through to other systems. The following gateway types are possible:

- NetWare mapped drives
- NetWare connected print ports
- LPRMON connected print ports
- LAN Server Peer connected print ports

The following gateway services are possible with the aid of additional software:

- NFS mounted drives
  - NFS kit for OS/2 including latest CSDs and APARs
- AS/400 PC Support connected drives
  - AS/400 Client Access or equivalent
  - Communications Manager/2

NetWare File and Print Gateway Services

OS/2 Warp Server is able to act as a File and Print Gateway to NetWare Servers. This means that an OS/2 Warp Server can share logical drives or print queues that are physically on a NetWare server. Requesters that are connected to the the OS/2 Warp Server can use these resources without having the NetWare requester installed on their machine. This setup may be required for one of the following reasons:

- This reduces the number of connections used on the NetWare Server.
- Only OS/2 Warp Server requester code needs to be maintained on each workstation. There is no need to install NetWare Client code on each machine thereby conserving workstation resources, such as disk and memory.
- When migrating from NetWare to OS/2 Warp Server this may be used as an interim step whilst the data is migrated.

Setting Up the NetWare File and Print Gateway

Figure 34 on page 34 depicts a simple scenario where OS/2 Warp Server is used as a file and print gateway to a NetWare Server.

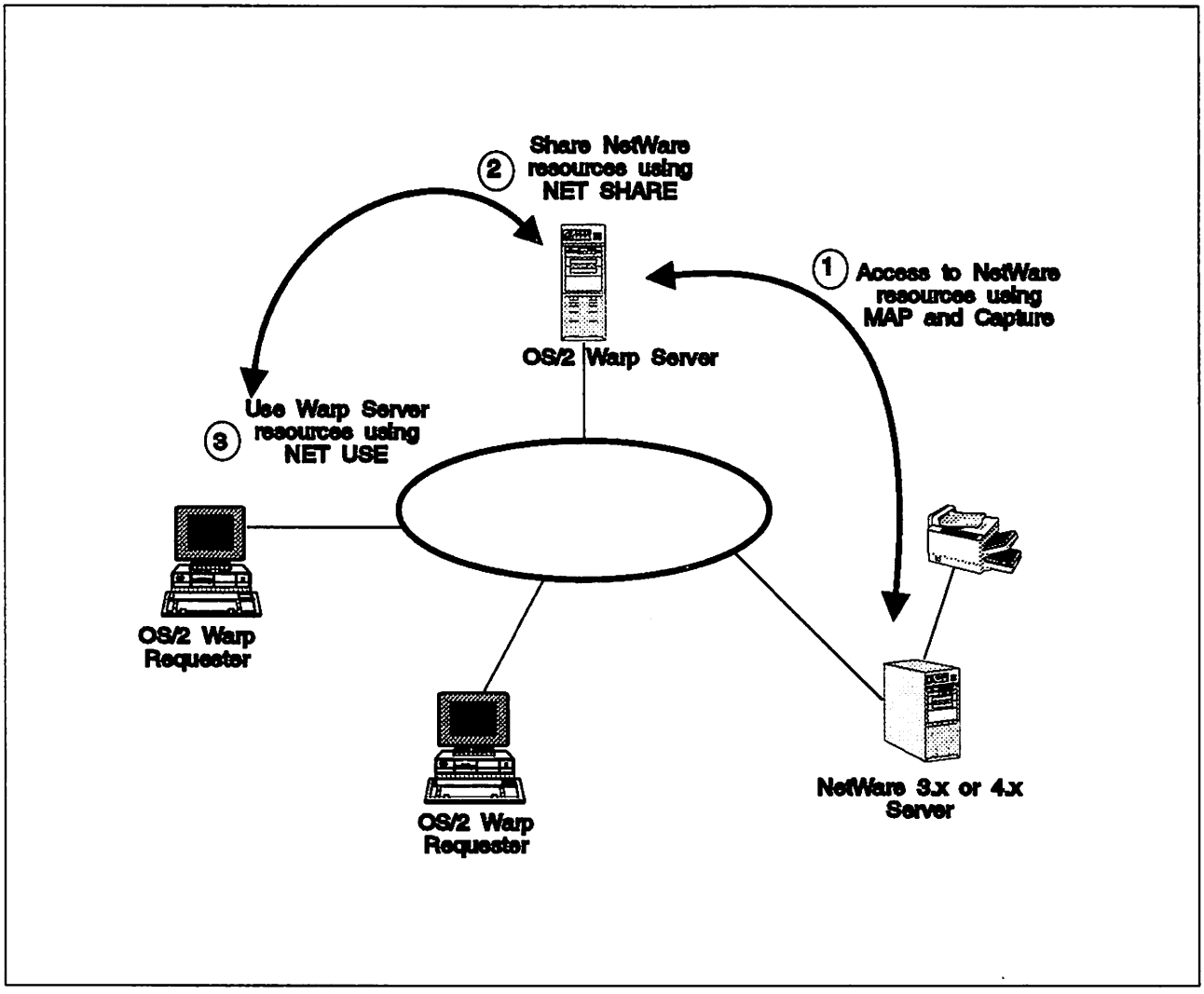


Figure 34. NetWare File and Print Gateway Services Overview

The steps, as shown in Figure 34, are:

1. From OS/2 Warp Server, you log on to the NetWare file server and gain access to resources by using the *Capture* and *Map* facilities.
2. You then issue a NET SHARE for the resources you gained access to in step 1. Optionally you could create aliases to define the resources.
3. Once the resources are shared, the file and print clients may access the resources by issuing NET USE commands, or have the resources assigned to them as logon assignments of current assignments (see "Connecting to Network Resources from the OS/2 File and Print Client" on page 62 for a discussion on the types of resource assignments).

In order to connect to the NetWare Server OS/2 Warp Server uses the NetWare Client for OS/2 Version 2.11. The version of the NetWare Client for OS/2 included in OS/2 Warp Server includes the fixes from the *OS2C1*. Some of the features of this Client are:

- Support for both NetWare 3.x and NetWare 4.x Servers
- Provides access for up to nine parallel ports
- Support for OS/2, DOS and WIN-OS/2 sessions

The DOS and WIN-OS/2 sessions can be set up for global or private support. Global support means that after logging in from a DOS VDM, other DOS VDM's are aware of the login. Private support means each VDM is unaware of any other login.

- Support for VMBoot private and Global sessions

  VMBoot is used for support of the NWAdmin utility (for administering a NetWare 4.x network).

In order to set up the File and Print services gateway you need to complete the following tasks:

- Install the NetWare Client for OS/2
- Configure the NetWare Client for OS/2
- Login and connect to resources on the NetWare server
- Configure the shares for use by OS/2 Warp Server requesters
- Automate the procedures

Installing the NetWare Client for OS/2: The NetWare client is part of the integrated installation if the File and Print services gateway option is selected as part of the OS/2 Warp Server installation process. Figure 35 shows the parameters that you are prompted for.

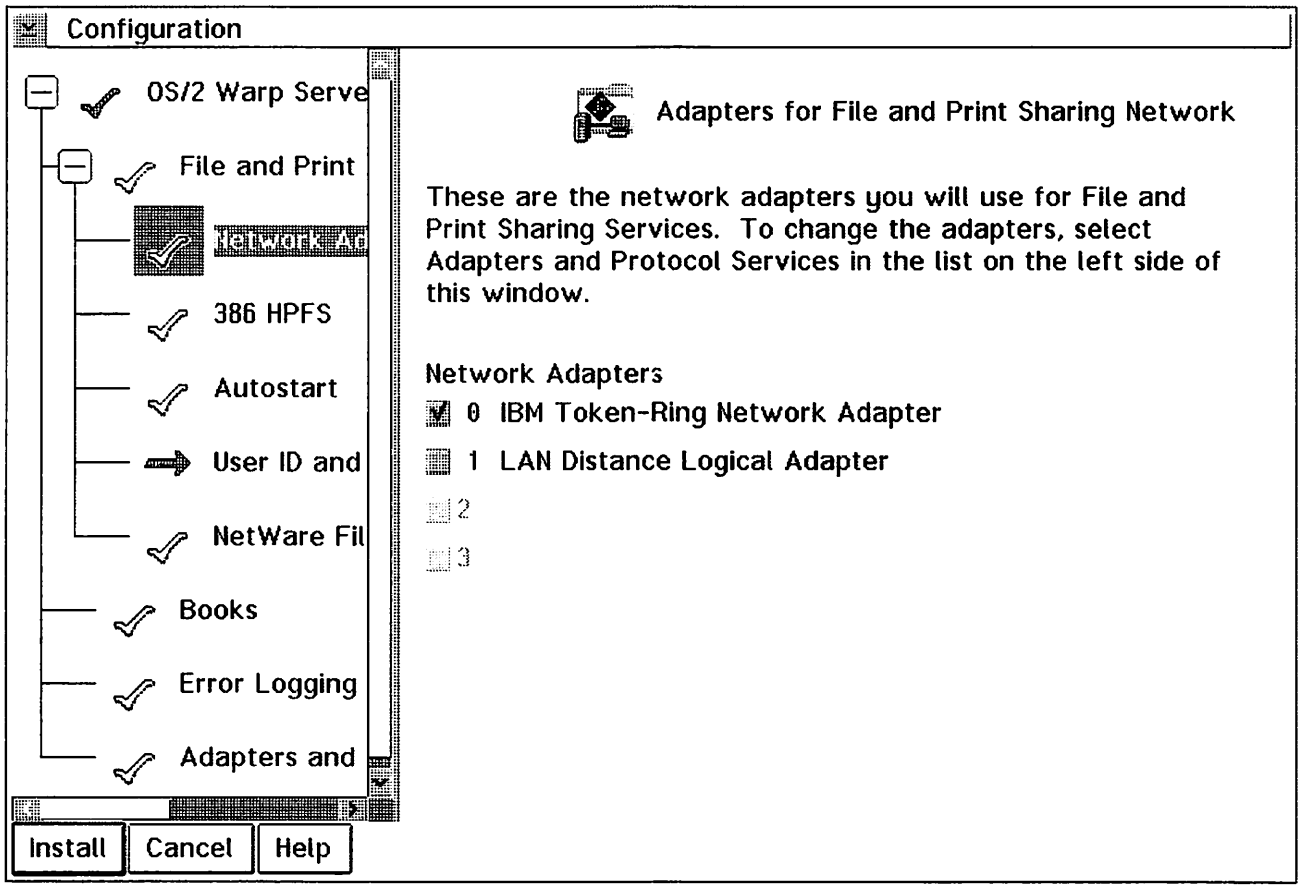


Figure 35. Integrated Installation - NetWare File and Print Services

- You are required to specify the drive on which the NetWare Requester will be installed

- The default server to make a connection to (optional)
- The network adapter that will be used to connect to the NetWare Server, notice that only the available adapters are selectable

If you choose to install the NetWare Client for OS/2 from the diskette images you will be prompted for more parameters. These are documented in the *NetWare Client for OS/2 Installation and Configuration* redbook.

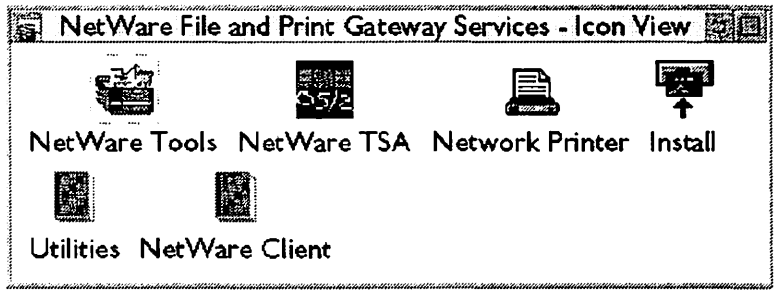


Figure 36. NetWare File and Print Services Folder

If you wish to reconfigure the NetWare Client you can run the installation Utility from the NetWare File and Print services folder. From the action bar, select the Installation pull-down menu. From the Installation pull-down menu select **Requester on workstation....** The options that you have are displayed in Figure 37

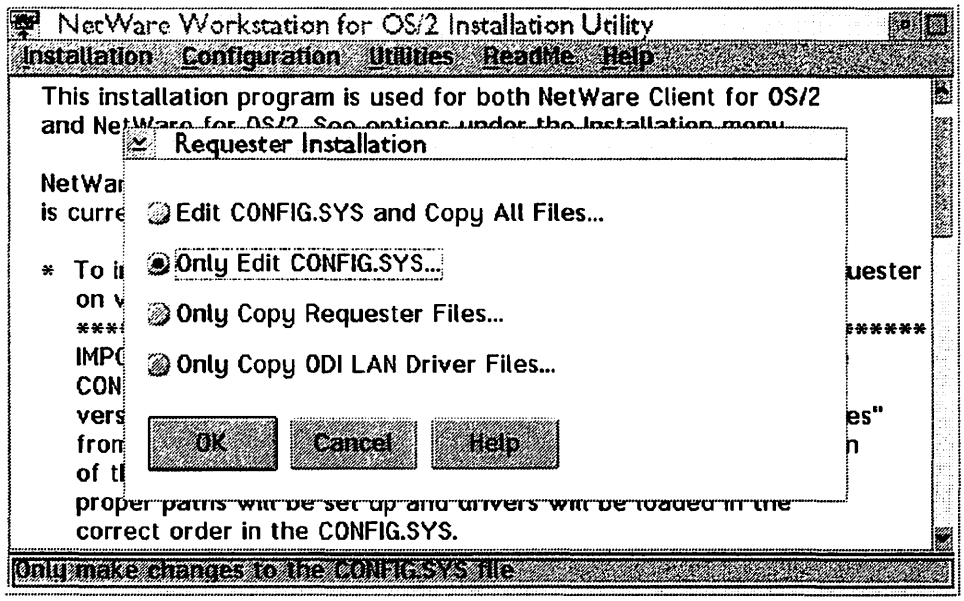

NetWare Workstation for OS/2 Installation Utility
Installation Configuration Utilities ReadMe Help
This installation program is used for both NetWare Client for OS/2
Requester Installation
Edit CONFIG.SYS and Copy All Files...
Only Edit CONFIG.SYS...
Only Copy Requester Files...
Only Copy ODI LAN Driver Files...
OK
Cancel
Help
correct order in the CONFIG.SYS.
Only make changes to the CONFIG.SYS file

Figure 37. NetWare Installation and Configuration Program

Since the requester is already installed this will provide you with the option to change CONFIG.SYS without copying the files over again.

Configuring the NetWare Client for OS/2

During the installation a default NET.CFG file is created with default settings. Usually the defaults should be fine for most installations however you may need to configure the NetWare Client if:

- Your workstation has more than one network adapter or the adapter is not using default factory settings
- Your network uses an Ethernet frame type other than Ethernet 802.2

Configuration may also be useful in these circumstances:

- If you want to change the default packet signature security level
- If you want to turn off Packet Burst or Large Internet Packet transmissions
- If the workstation will connect to a token-ring network using source routing
- If the workstation will use NetBIOS or Dual NetBIOS protocols
- If the workstation will use Named Pipes protocol
- If you want your workstation to connect to a preferred Directory tree
- If you are setting up Remote Program Load (RPL) workstations
- If you want to change your default login drive

To reconfigure the NetWare client you will need to use the Install icon located in the Novell folder on your desktop. See Figure 37 on page 36. Alternatively you may edit the NET.CFG file that is in use using a text editor such as E or EPM. The NET.CFG file is a text file that contains your tailored configuration options. When you start up your workstation the NetWare Client for OS/2 searches for a NET.CFG in the directories specified in the DPATH line in the CONFIG.SYS. If the Client does not find a NET.CFG it starts up using the default values built into the software.

Connecting to resources on the NetWare Server: You should now have access to a NetWare Server. You may log in the server either from the command line or from the NetWare Tools program which is in the Novell folder on your desktop. The difference between the two is that the command line utility runs a login script. Login from the Tools program does not run a login script.

To login from an OS/2 command prompt enter:

```
login username
```

To log in using your username to a specific server, type:

```
login servername/username
```

You will then be prompted for a password.

The NetWare Tools allows you to do the following:

- Manage drive mappings
- Manage printer connections and setup
- Manage directory tree and server connections
- Display network users
- Send messages

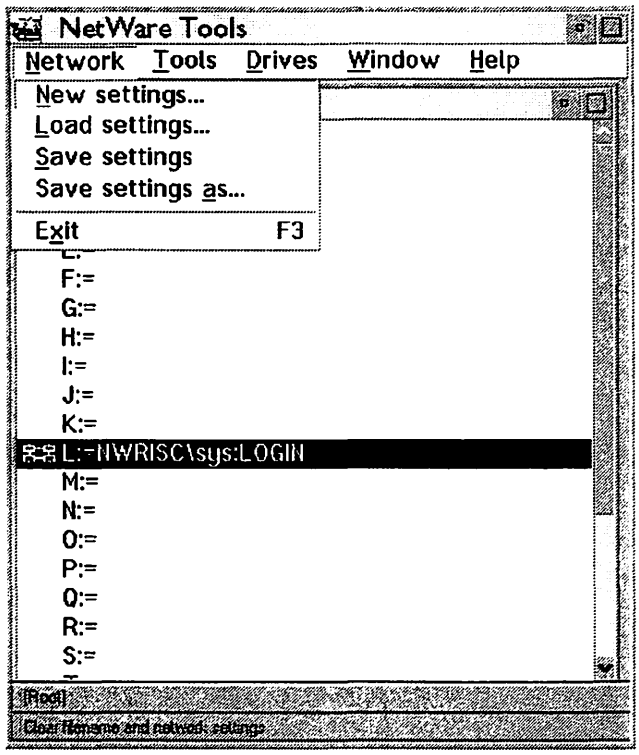


Figure 38. NetWare Tools Network Option

Note: Choosing the **Settings** option disconnects all current server connections. Make sure that all open files and applications are closed.

To login to a NetWare Server from the Tools program choose the server option off the Tools Menu. After doing this a Server Menu Item appears on the Action bar. Choose the Attach option of this menu to attach to a server. You will be prompted for the Server, Username and Password.

Mapping a Drive: Once you have logged on you may now map your local drive letters to the NetWare Servers directories. By double clicking on a drive within your NetWare Tools folder you will be presented with a MAP selection window as shown in Figure 39 on page 39. In the figure the user is not logged on so no volumes or directories are shown. An attach button allows you to logon into another NetWare Server.

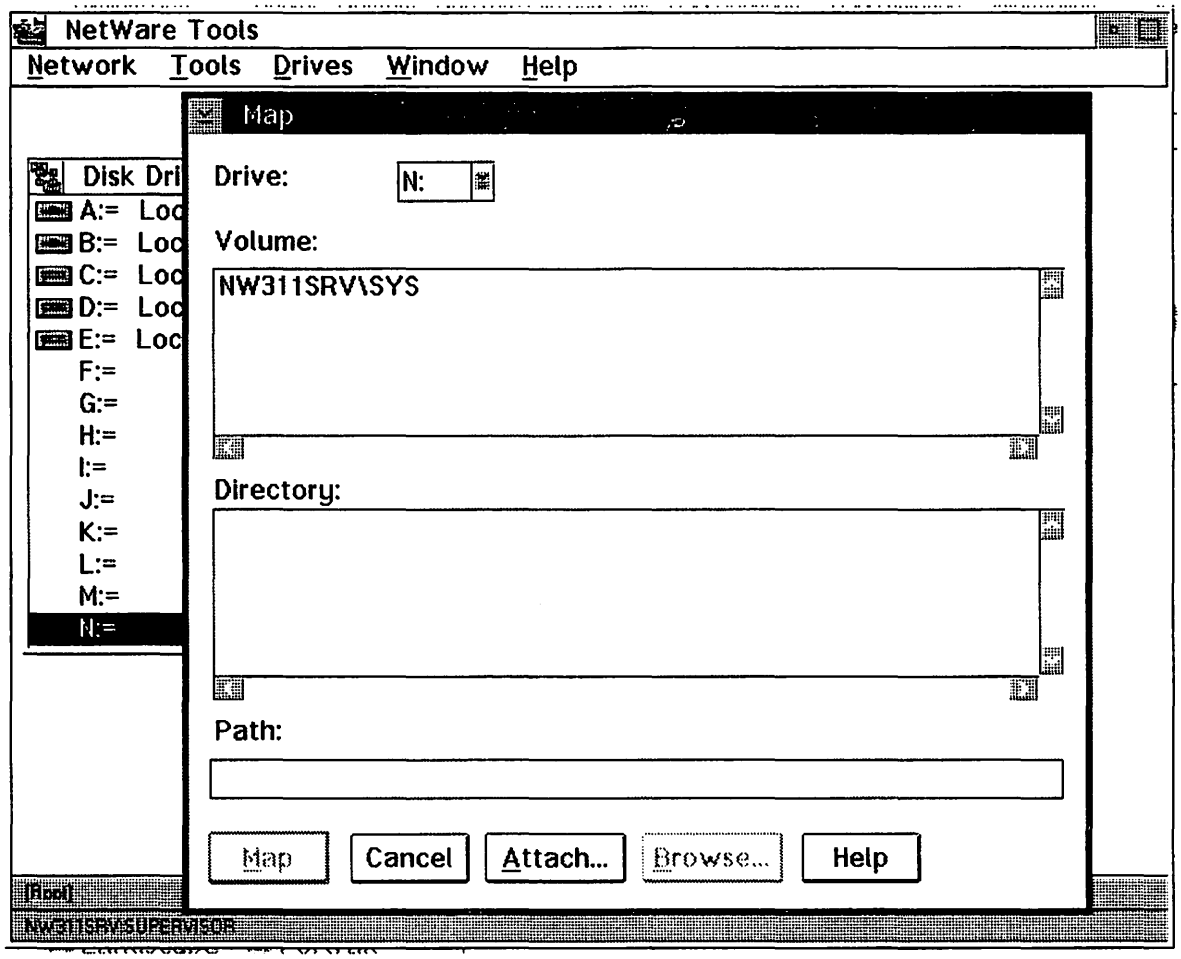


Figure 39. NetWare Tools, Mapping a Drive

Once you have logged on, select a free drive by double clicking on it within the drives window. You will be presented with a window that allows you to select the volume and the directory within the volume. If the drive that you wish to attach to is on a another server, select the attach button to attach to that server.

The NetWare requester for OS/2 also has a command line option that allows you to map drives from the command line. The syntax of the MAP command is:

```
MAP[option¦/VER][drive:=][path]
```

Where the options are:

- DEL - to delete a drive mapping
- N - to map the next available drive
- P - to map a drive to a physical volume on a server
- /VER - to display the version information

For example to map the next available drive to the login directory on server ITSO use the command:

```
MAP N:=ITSO/SYS:LOGIN
```

To delete the above drive mapping you would use the command:

```
MAP DEL N:
```

To map drive M: to SYS:PUBLIC use the command:

```
MAP M:=SYS:PUBLIC
```

Setting up a Print Queue: In order to redirect print queues from your workstation to a NetWare server you will need to select the Printers option on the Tools Action list.

A Printer Ports window will be displayed. You can select a port by double clicking on it or by selecting the Capture option of the Printers action item capture all output from a *local printer* port to a NetWare Print Queue. You will be presented with the options as shown in Figure 40.

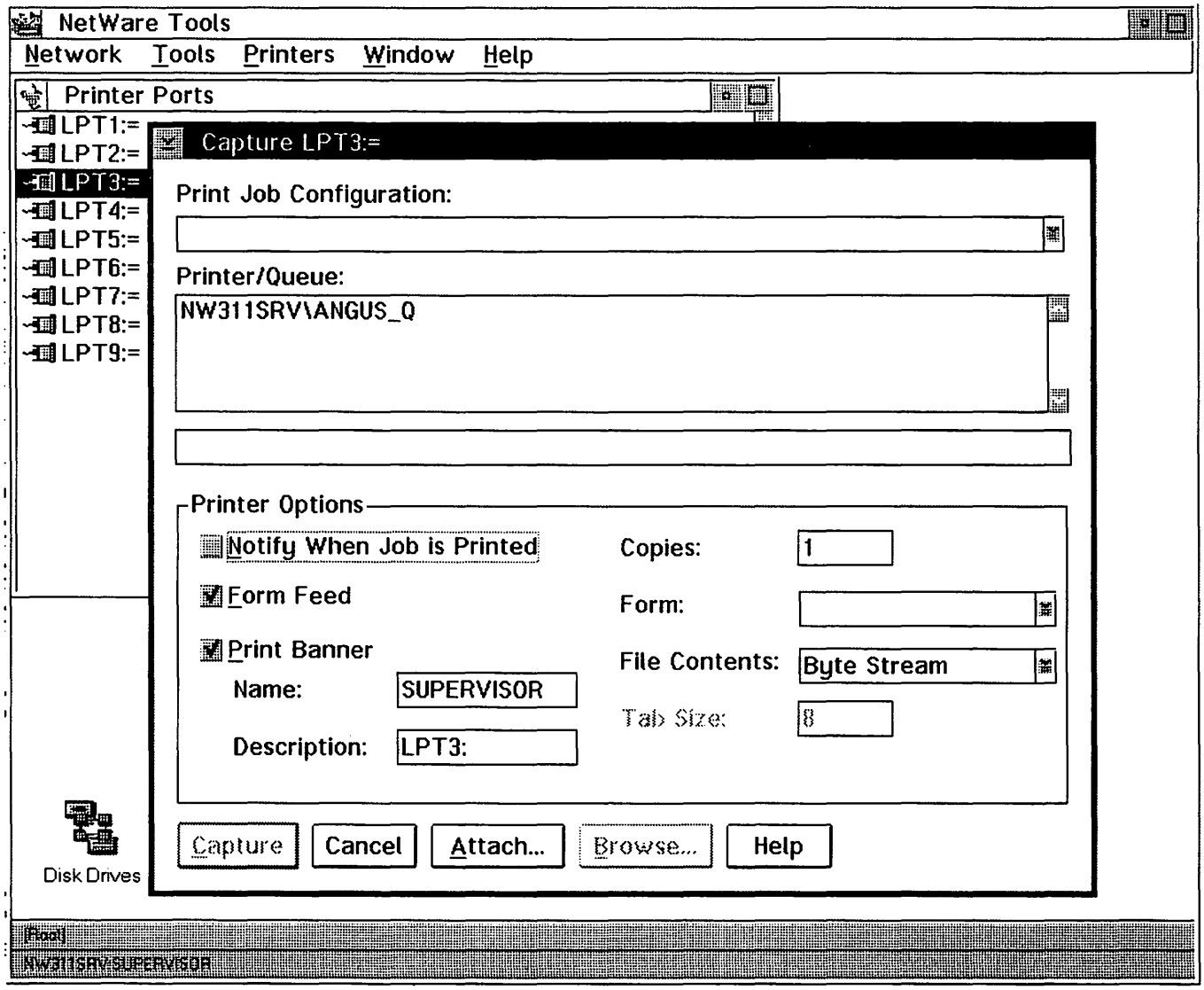


Figure 40. NetWare Tools, Capturing a Printer Port

The following options are available:

Option	Function
Notify	Confirms print job completion
Form Feed	Places a page break between print jobs

Copies	Specifies the number of copies to print
Tab Size	Specifies the number of characters in a tab stop
File Contents	Specifies the type of print file being printed
Print Banner	Allows for a banner page to be printed at the front of your print job
Form	Allows you to select a defined print form

Once all settings for drives and print queues being shared are defined, they need to be saved. To do so select the Network pull-down menu from the NetWare Tools action bar and select *Save Settings* (See Figure 38 on page 38). You will be prompted for a file name. The default extension for this file is NWS.

Configuring the shares for use by OS/2 Warp Server requesters: To configure the logical drive and print queue you need to logon to LAN Server as an administrator. Once you are logged on there are a number of methods that you can use to share the resources.

You can share the resources using the NET SHARE command or you can create an alias to define the resource. However, it might be best to use the NET SHARE command as the NetWare server may not always be available.

For example, to share the N drive to an unlimited number of users with read and execute access, you would issue the command:

```
NET SHARE NETWARE=N: /UNLIMITED /PERMISSIONS:RX /REMARK:NWare Drive
```

Access Control: Since the drive being shared is a logical drive there are two access control mechanisms in place. These access control mechanisms work independently from each other. Checking is done at each access control point. The first access control mechanism is present at the NetWare server. The user ID used to log on to the NetWare server from the OS/2 Warp Server can have any of the following rights defined on a resource:

- S - Supervisory
- R - Read
- W - Write
- C - Create
- E - Erase
- M - Modify
- F - File Scan
- A - Access Control

The NetWare access control mechanism will ensure that these rights are preserved. These rights only apply to the user ID logged on at the OS/2 Warp Server gateway machine.

LAN Server is provides the second access control mechanism. These access controls will apply to the user IDs logged on at the OS/2 Warp Server clients. LAN Server allows the following access controls to be defined for a shared resource:

- X - Execute

- R - Read
- W - Write
- C - Create
- D - Delete
- A - Attributes
- P - Permissions

When an OS/2 Warp Server client attempts to gain access to the double redirected resource the success or failure of the attempt will be determined as follows:

1. First, when a user attempts to access the resource, the LAN Server access control mechanism will check if the the user has the appropriate rights. These rights will have been defined using the NET SHARE, NET ACCESS commands or from the Administration GUI.
2. If the user does not have appropriate access permission the attempt will fail. If the user does have appropriate access permission the request will be passed on to the NetWare server.
3. Checking on the NetWare server will be done using the user ID logged on to the NetWare server from the OS/2 Warp Server gateway machine and not the user ID at the client workstation.
4. If the user has sufficient access, access is granted and the user can make the changes they want. If the user does not have appropriate access permission an error message will be displayed.

Automating the Process: The above procedure has to be followed each time the NetWare or LAN Server machine is restarted. In order to make this process less cumbersome it is best to automate it.

You can automate the login process to the NetWare server by doing the following:

- Map all the drives you need
- Capture any printer ports needed
- Save the setting to a file, for example, LOG.NWS, the .NWS (for NetWare Settings) extension is automatically added
- Add the following to the STARTUP.CMD

```
NWTOOLS.EXE LOG.NWS AUTOEXIT
EXIT
```

- Add the following lines to the end of the CONFIG.SYS file:

  Note: The user ID that is used to log in to the NetWare server should not have the password enabled. Having the password enabled will stop the login process.

```
CALL=C:\NETWARE\NWSTART.EXE
CALL=C:\NETWARE\LOGIN.EXE server/user
```

You will also need to automate the LAN Server logon and resource sharing. This can be done by:

1. Logon to the server

   Add the following line to STARTUP.CMD after the NET START SERVER command:

```
logon userid /p:password
```

Where `userid` is a valid administrator user ID and `password` is the password corresponding to this user ID.

2. Share the resources

   Use the `NET SHARE` command to share the resource.

Considerations

The following limitations exist when using the NetWare File and Print Gateway:

- Authentication between the gateway server and the remote server is done on the basis of the user logged on at the server or the workstation ID of the server, depending on the protocol. The identification of the client originating the request is not forwarded through the gateway.
- The machine acting as the NetWare gateway will have to remain logged on to a NetWare server while these services are in use. The machine will have to be secured by a lockup password or equivalent.
- Only job submission is supported through the gateway. Printer management, job management and queue management will not work and are not supported. Alerts generated for the print jobs by the remote server will be sent to the gateway server and will not be forwarded on.

TCP/IP Services Interoperability

This section will describe how to use TCP/IP Services in conjunction with other components of OS/2 Warp Server in order to provide access to TCP/IP networks for clients that do not have any TCP/IP capabilities on their own.

Using OS/2 Warp Server as a TCP/IP File Sharing Gateway

File and Print Sharing Services of OS/2 Warp Server not only enables you to share files and directories that reside on the server itself, but it also allows you to share network resources that actually reside on remote systems. This is sometimes called the *double redirection technique*. The following provisions on how this can be done should be considered:

- You cannot double-redirect OS/2 Warp Server or OS/2 LAN Server file resources with File and Print Sharing Services; you have to set up cross domain aliases.
- You need to install the appropriate client software on your OS/2 Warp Server system in order to connect to the remote file server.
- Being a client to that remote server, you need sufficient permissions to access the shared resources.

One way of implementing that kind of a file sharing gateway with OS/2 Warp Server can be accomplished by having OS/2 Warp Server act as a NFS client. OS/2 Warp Server can then share NFS-mounted drives for any LAN Requesters that are connected to it but which do not have NFS client capabilities of their own. Please see "Network File System (NFS) Services" on page 246 for more information on how to integrate the NFS client at the OS/2 Warp Server. Figure 41 on page 44 shows a scenario for a TCP/IP file sharing gateway.

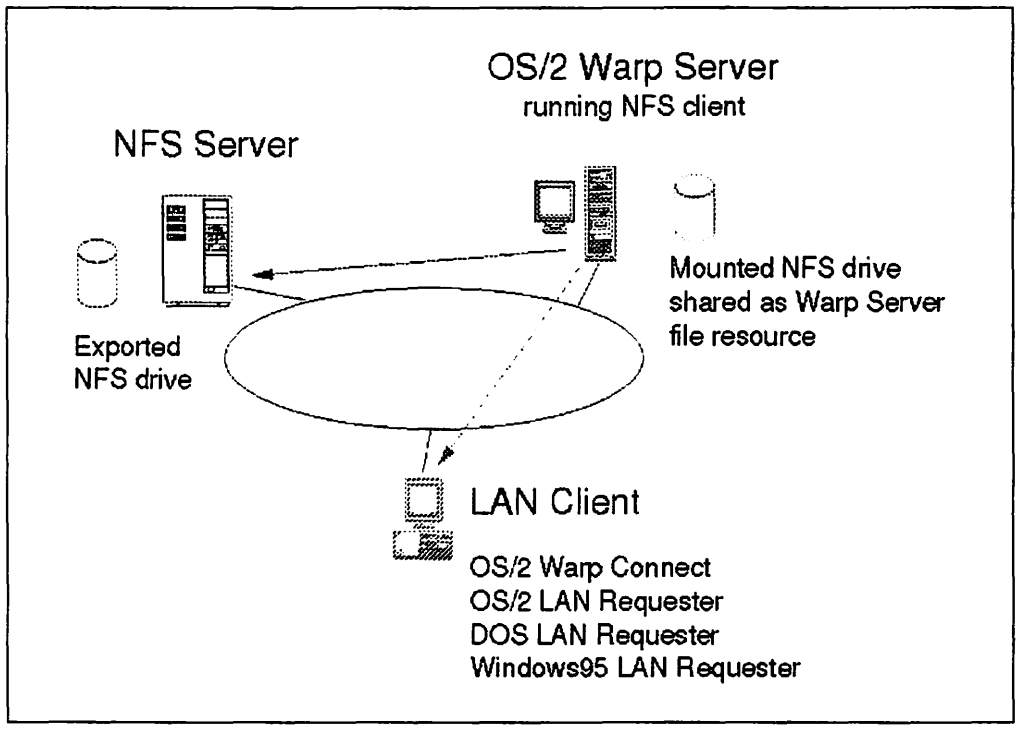


Figure 41. TCP/IP File Sharing Gateway

Please see Chapter 2, "File and Print Sharing Services" on page 7 for more information about how to share file resources.

Access Permissions, Case Sensitivity, and File Locking: Three issues must be addressed when discussing double-redirection of NFS-mounted drives with OS/2 Warp Server:

Access Permissions: NFS itself does not provide for access permissions for files or directories like OS/2 Warp Server does with File and Print Sharing Services. NFS can only restrict access to an exported directory to a list of clients, and it can allow for read-only or for write access. Any further detailed access protection scheme is up to the underlying operating system or file system.

When an NFS client attaches to a server, the client name will first be checked against the export list. If the names match, the user at the client system has to identify himself, and based on this information, access to the exported file or directory may be restricted further. Let's consider the following:

Example: In the case of a UNIX NFS server, a client system (`joes-pc`) may be listed for read access in the export list, and that is all that NFS requires.

```
# export list for sample NFS server
# directory    NFS permissions    Export list

/u/joe         rw                 joes-pc franks-pc carries-pc
```

If the user (`Bill`) at that client authenticates himself properly to UNIX (*not* to NFS!), he will be able to mount the requested directory.

```
user:      bill
password:  ******
UNIX user ID:   102
UNIX group ID:  201
UNIX group:     clerks
```

What that user can actually do to that resource is limited to the permissions defined within the UNIX file system, which is totally outside the control of NFS.

```
-rwxr-x---   1 joe      janitors    1853 Sep 22 18:17 Mwm
-rw-rw----   1 joe      janitors      47 Sep 22 18:17 Xant
-rw-rw----   1 joe      janitors   16387 Sep 22 18:17 Xmh
-rw-r-----   1 joe      janitors    1940 Sep 22 18:24 smit.log
-rw-r-----   1 joe      janitors       0 Sep 22 18:23 smit.script
```

In this case, user `Bill` would not be able to do anything on `/u/joe` because he is neither the owner of the resource, nor is his group, or anyone else, allowed access.

For the purpose of this scenario, you should first determine what access permissions the clients desire at the remote file server. Then log on from the OS/2 Warp Server NFS gateway with a user ID that has sufficient permission at the NFS server system to satisfy those requirements. You can, of course, limit the access permissions of that user for the clients using File and Print Sharing Services access profiles.

Case Sensitivity: Since many NFS servers actually run on UNIX or UNIX-like systems, there may be problems with file names in upper, lower or mixed case. The UNIX file system, and probably others as well, will treat any file name spelled in different cases as different files, as shown in the following example:

```
FileName
FILENAME
filename
```

Since the OS/2 HPFS file system itself is not case-sensitive to file names, the names in the above example would result in one and the same file, no matter how they are spelled. The name actually used for a file would be the first one ever given to it. The OS/2 FAT file system only uses uppercase file names that comply with the 8.3 convention (eight character file name, separation period, three character extension).

This leads to the question of how clients that use OS/2 Warp Server as an NFS gateway will be able to differentiate between files at the NFS server which have the same name, but are spelled in different ways. To overcome this, the OS/2 NFS client (which would run on the OS/2 Warp Server system) can be configured to respect case sensitivity by starting it with the `-c` and `-z` options.

Note: Since OS/2, which provides the underlying file system, is not case sensitive, an OS/2 NFS server will not recognize case sensitive file names.

File Locking: An NFS server does not provide file locking capabilities, as strange as that is in a file sharing environment. This function is left to the NFS clients. The OS/2 NFS client will respect file and record locking if SUN Lock Manager is installed and running at the NFS server system.

Using OS/2 Warp Server as a TCP/IP Remote Printing Gateway

File and Print Sharing Services of OS/2 Warp Server not only enables you to share printers that are attached to the server itself, but it also allows you to share printers that actually reside on a remote system. This is another kind of double redirection technique. The following provisions on how this can be done should be considered:

- You need to install the appropriate client software on your OS/2 Warp Server system in order to connect to the remote print server.
- Being a client to that remote server, you need sufficient permissions on the shared resources in order to allow clients to access print queues on the remote server.

One way of implementing that kind of a remote printing gateway with OS/2 Warp Server can be accomplished by having OS/2 Warp Server act as a TCP/IP line printer client. OS/2 Warp Server can connect to TCP/IP printers by using either the LPRMON or the LPRPORD function provided in TCP/IP Services. OS/2 Warp Server can then share printers for any LAN Requesters that are connected to it but which do not have TCP/IP capabilities of their own. Figure 42 shows a scenario for a TCP/IP remote printing gateway.

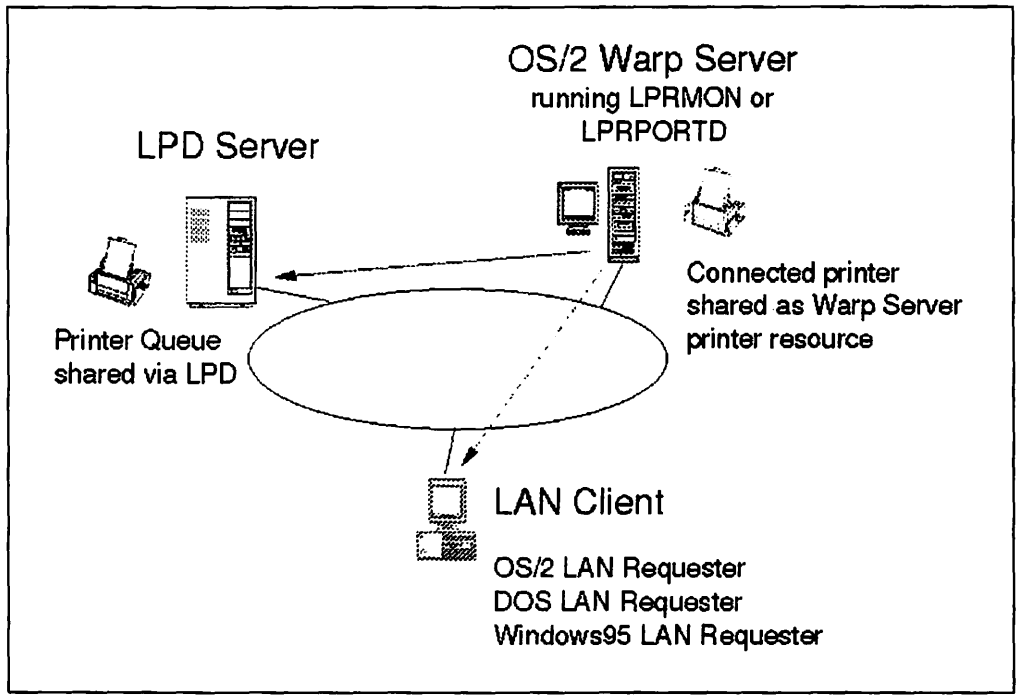


Figure 42. TCP/IP Remote Printing Gateway

Please see Chapter 2, "File and Print Sharing Services" on page 7 for more information about how to share printer resources.

Using OS/2 Warp Server as a Communications Gateway for Internet Access

The File and Print Sharing Services of OS/2 Warp Server allow you to share a serial interface (COM port) over the LAN so that users from other workstations can access any devices attached to that port at a server. By making use of this capability of OS/2 Warp Server, you can support a group of LAN users with Internet access without the requirement of having a modem and telephone line available to each of them.

You need to have File and Print Sharing Services installed at the server, and you need either an OS/2 Warp Server client, OS/2 Warp Connect or OS/2 LAN Requester Version 3.0 and above in order to access a shared COM port for the IBM Internet Connection.

Note: You also need to register each user for Internet access, for example with the IBM Internet Connection, because it is the user's client that actually

performs the dial-up to the Internet service provider, even if the server's COM port is used. The server does not require any specific Internet connectivity at all, just a modem and a telephone.

Please refer to *Network Administrator's Reference Volume 3: Network Administration Tasks* for more information about how to share a serial port over the LAN. Figure 43 shows a scenario of shared COM ports for Internet access.

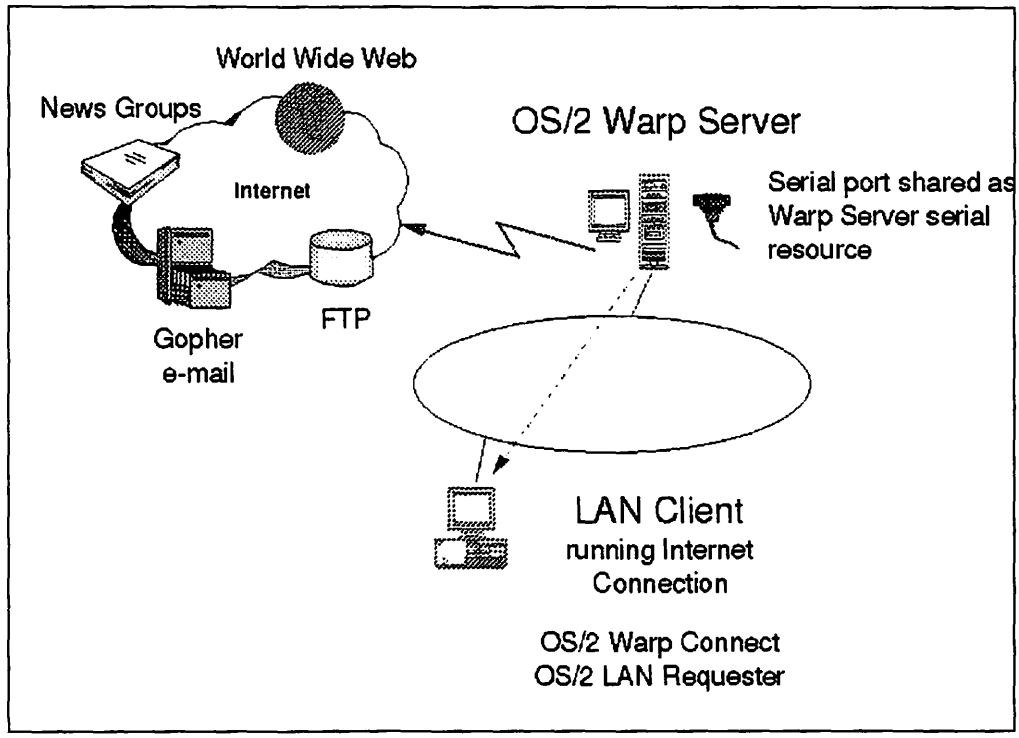


Figure 43. Internet Access via Shared COM Ports

Chapter 3. File and Print Clients

In OS/2 Warp Server the OS/2 file and print client, also called requester, has some minor functional enhancements over the OS/2 LAN Requester shipped with OS/2 LAN Server 4.0. DOS LAN Services, however, features a large number of enhancements. Therefore, much of this chapter will concentrate on the DOS, Windows and Windows 95 clients.

In Chapter 2, "File and Print Sharing Services" on page 7 we looked at how to share resources in an OS/2 Warp Server environment. In this chapter we will look at how users connect to these shared resources.

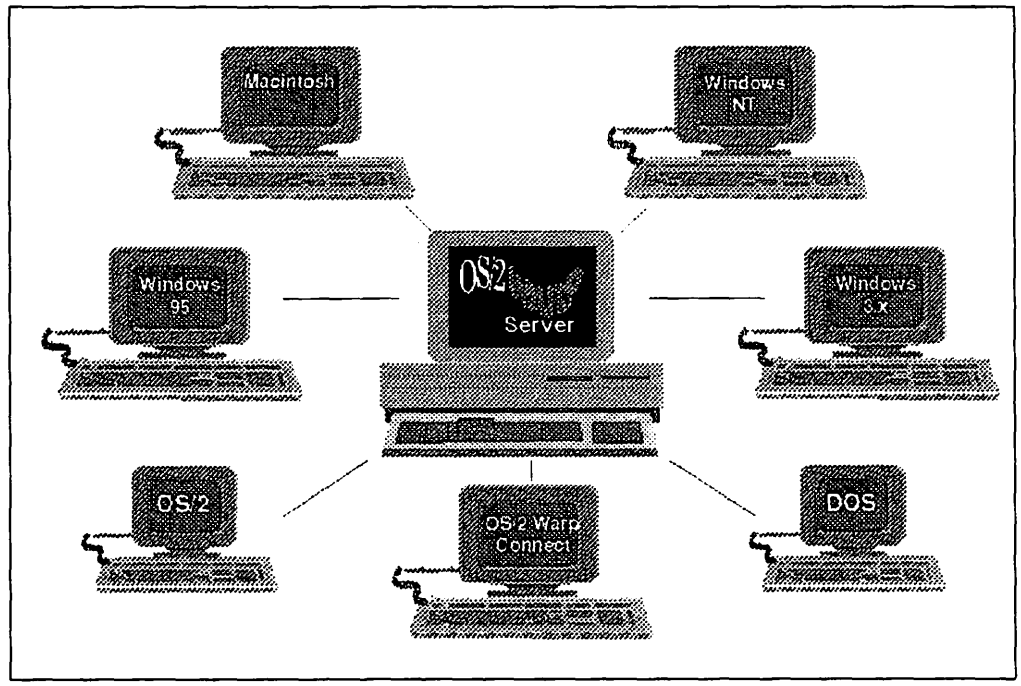


Figure 44. Client Machines (Requesters) Supported By OS/2 Warp Server

OS/2 Warp Server supports a broad range of clients by providing requester code to match and integrate with the most common workstation operating system environments. OS/2 Warp Server is also backward compatible with previous OS/2 LAN Server clients which allows you to incrementally add OS/2 Warp Server servers to an existing LAN Server network and provide complete compatibility between systems.

The following requesters are provided with OS/2 Warp Server:

- OS/2 Client (OS/2 LAN Requester)
- DOS Client (DOS LAN Services)
- Windows Client (DOS LAN Services Windows Support)
- Windows 95 Client (DOS LAN Services for Windows 95)

Note: In addition, OS/2 Warp Server supports (but does not include) Windows for WorkGroup and Windows NT clients connecting to OS/2 Warp Server shared resources. The Novell NetWare Requester for OS/2 is included to provide a gateway to resources located on NetWare servers (see 2.10, "OS/2 Warp Server

© Copyright IBM Corp. 1996

Gateway Services" on page 32). Macintosh clients are supported via IBM's LAN Server for Macintosh add-on product which is available separately.

3.1 What is a Requester?

Before looking at what each requester provides in terms of features and functions it is important to understand the purpose of a requester.

A *requester* is a workstation from which you can log on to a domain or access a server (IBM or non-IBM) and use resources. After successful logon it is possible to access shared resources and use the processing capability of the servers. Because you can access shared resources from requesters, you can reduce your hardware requirements for the requester workstations.

There are three main types of requesters, or clients, in the IBM OS/2 LAN environment:

OS/2 LAN Requester: An OS/2 workstation with requester functions of the OS/2 Warp Server product installed and running.

DOS Requester: A workstation with DOS LAN Services installed and running (see 3.3, "DOS File and Print Client (DOS LAN Services)" on page 64). You can install DOS LAN Services on a workstation running DOS with or without Windows. A version of DOS LAN Services is also provided with OS/2 Warp Server for workstations running Windows 95, we look at this in 3.5, "Windows 95 Client (DOS LAN Services for Windows 95)" on page 87).

Peer Workstation: This is a special type of requester. Like a server, a peer workstation shares it's resources with users on a LAN (see 3.9, "Sharing Requester Resources with the Peer Service" on page 96). A peer workstation can also be used as a requester.

3.2 OS/2 File and Print Client (OS/2 LAN Requester)

The OS/2 LAN Server 4.0 Requester is the component of OS/2 Warp Server that provides LAN connectivity for workstations running OS/2. It is also available as a component of both the OS/2 Warp Connect and OS/2 LAN Server 4.0 products.

The main features and functions of the OS/2 LAN Requester are:

- Graphical user interface (GUI)
- Access to network resources
- Network messaging
- Network DDE and Clipboard
- API support
- Connectivity with other network programs

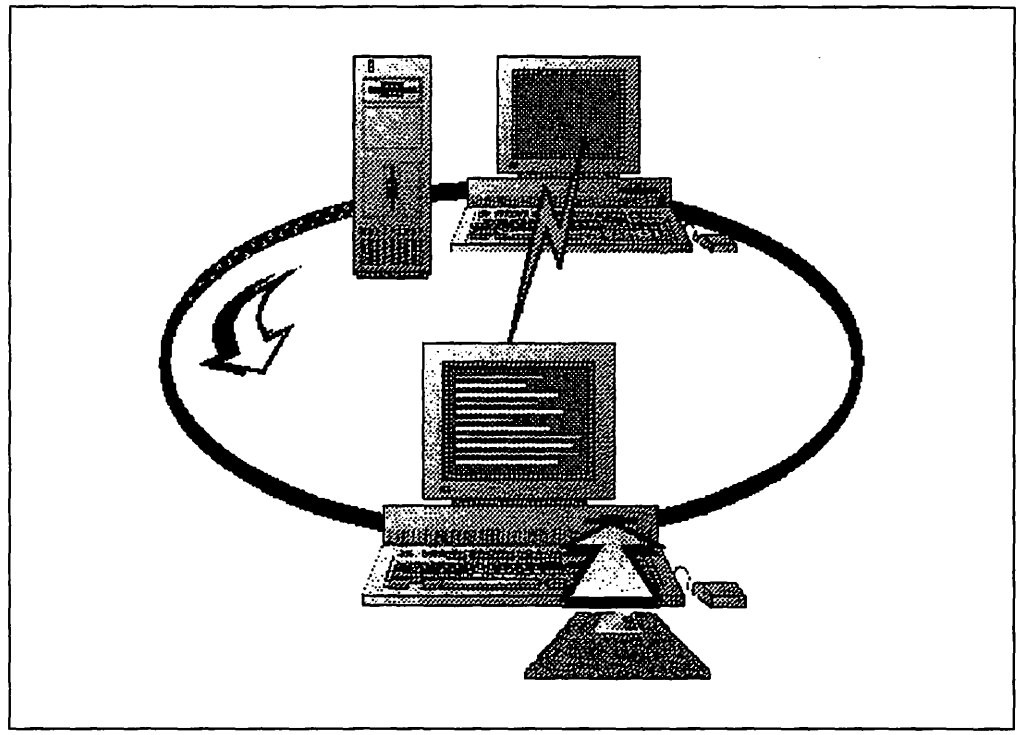


Figure 45. OS/2 Warp Server Client Installation

OS/2 Warp Server provides you with a number of options to install clients:

Across the LAN: Select this installation option where your clients do not have a CD-ROM attached. If you select this installation path you must:

1. Prepare your server workstation for client installation, which includes the creation of client remote installation diskettes, and is described in 2.8, "Preparing the Server for Client Installation" on page 28.
2. Restart the remote client with the Remote Installation Diskettes that you generated as part of the server preparation procedure.

   Remote Installation Prerequisites

   You *must* already have OS/2 version 2.0, 2.1, 2.11 or OS/2 Warp (with WIN-OS2) installed on the client in order to install any of the OS/2 clients.

3. If the installation program detects that OS/2 Warp is already installed on the workstation it prompts you to specify whether you wish to reinstall OS/2 Warp with networking support, or only install networking support.

   If you have multiple copies of OS/2 Warp installed on your system, for instance where you have different bootable partitions for whatever reason, you will be asked to select a version of OS/2 Warp to use for networking support.

4. After removing the remote installation diskette the workstation will restart and, if selected, will install the OS/2 Warp Server and then the OS/2 Warp Server installation program. If you select to reinstall OS/2 Warp and wish to retain existing programs, data and system configuration then you must

obviously *not* format the partition and ensure that the appropriate check boxes are selected on the Advanced Options screen.

5. After completing the fields in the Welcome to OS/2 Warp Server Installation window, as shown in Figure 3 on page 11, you are then asked whether you would like to install each of the client components, which are:

   OS/2 File and Print Client
   Remote Access Client
   TCP/IP Client
   System Management Client

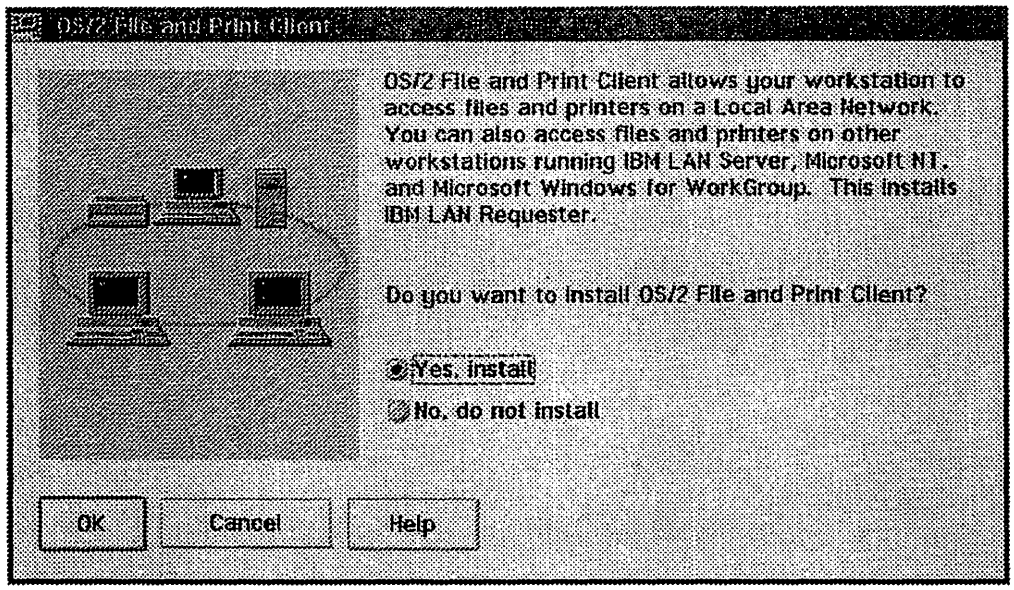

OS/2 File and Print Client
OS/2 File and Print Client allows your workstation to access files and printers on a Local Area Network. You can also access files and printers on other workstations running IBM LAN Server, Microsoft NT, and Microsoft Windows for WorkGroup. This installs IBM LAN Requester.
Do you want to install OS/2 File and Print Client?
Yes, install
No, do not install
OK
Cancel
Help

Figure 46. OS/2 File and Print Client Installation

The OS/2 File and Print Client is equivalent to the OS/2 LAN Requester provided with OS/2 LAN Server 4.0. We will look at the integral Administration Graphical User Interface in "Graphical User Interface" on page 60.

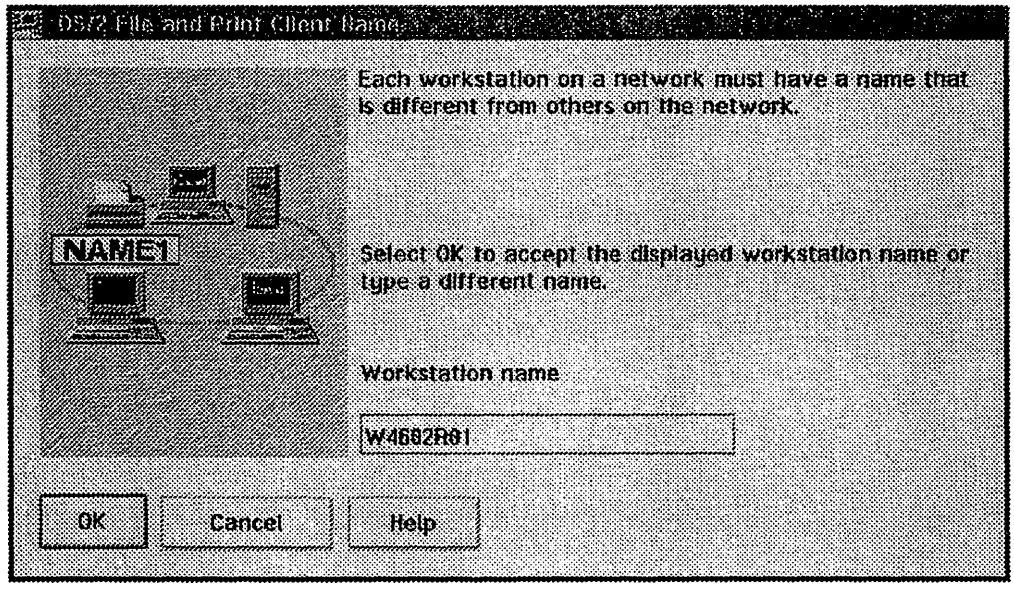

OS/2 File and Print Client
Each workstation on a network must have a name that is different from others on the network.
NAME1
Select OK to accept the displayed workstation name or type a different name.
Workstation name
W4682R01
OK
Cancel
Help

Figure 47. OS/2 File and Print Client Installation - Workstation Name

You must specify a name for the workstation which must be unique on the LAN and may be up to 15 characters in length. This is the equivalent of COMPUTERNAME in OS/2 LAN Server.

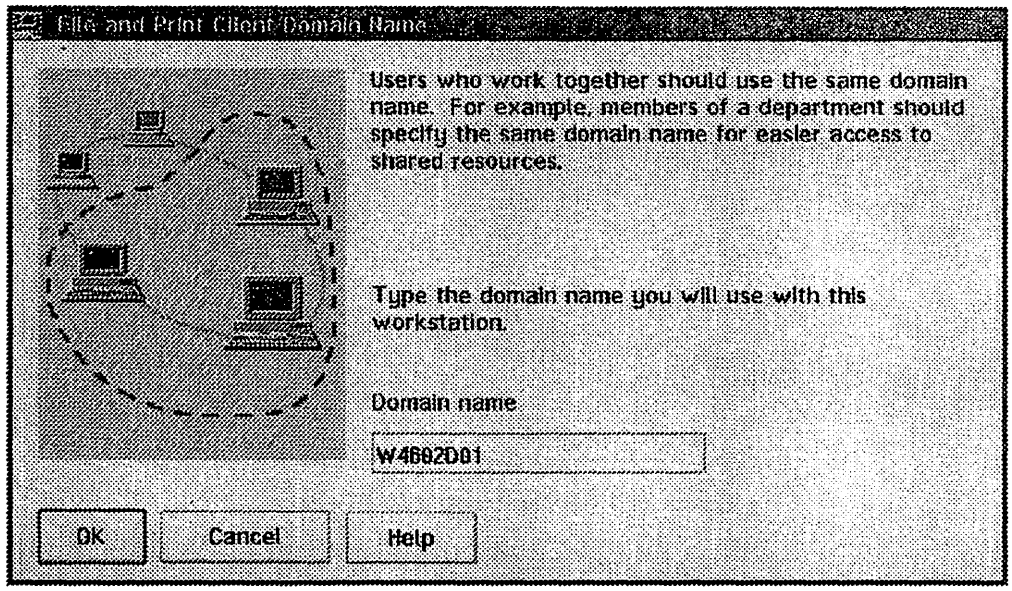

File and Print Client Domain Name
Users who work together should use the same domain name. For example, members of a department should specify the same domain name for easier access to shared resources.
Type the domain name you will use with this workstation.
Domain name
W4602D01
OK
Cancel
Help

Figure 48. OS/2 File and Print Client Installation - Domain Name

You must specify the domain that the workstation belongs to. This completes the information that you need to provide in order to configure the OS/2 file and print client.

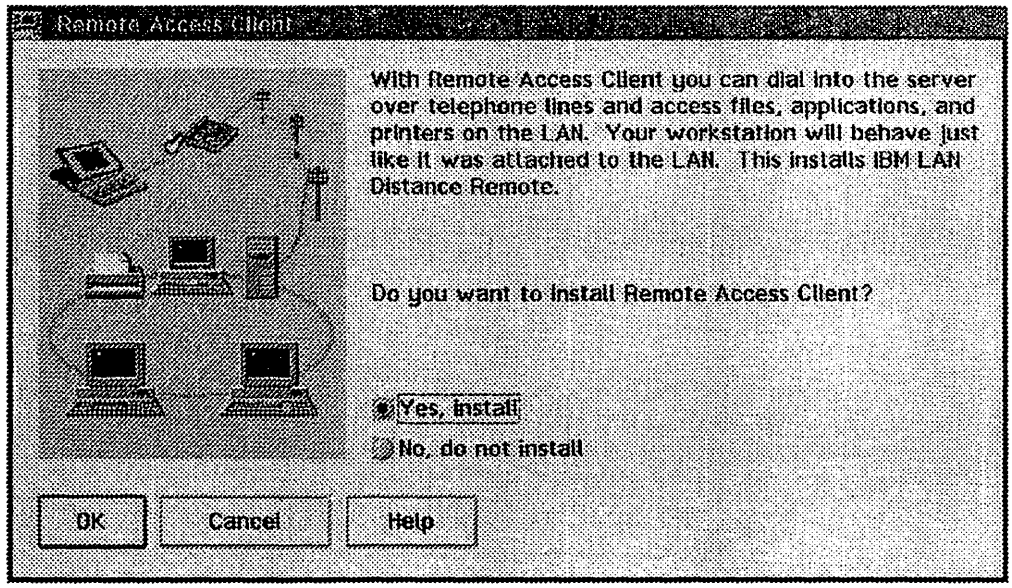

Remote Access Client
With Remote Access Client you can dial into the server over telephone lines and access files, applications, and printers on the LAN. Your workstation will behave just like it was attached to the LAN. This installs IBM LAN Distance Remote.
Do you want to install Remote Access Client?
Yes, install
No, do not install
OK
Cancel
Help

Figure 49. Remote Access Client Installation

The remote access client is the equivalent of the LAN Distance Remote client. Installation is optional.

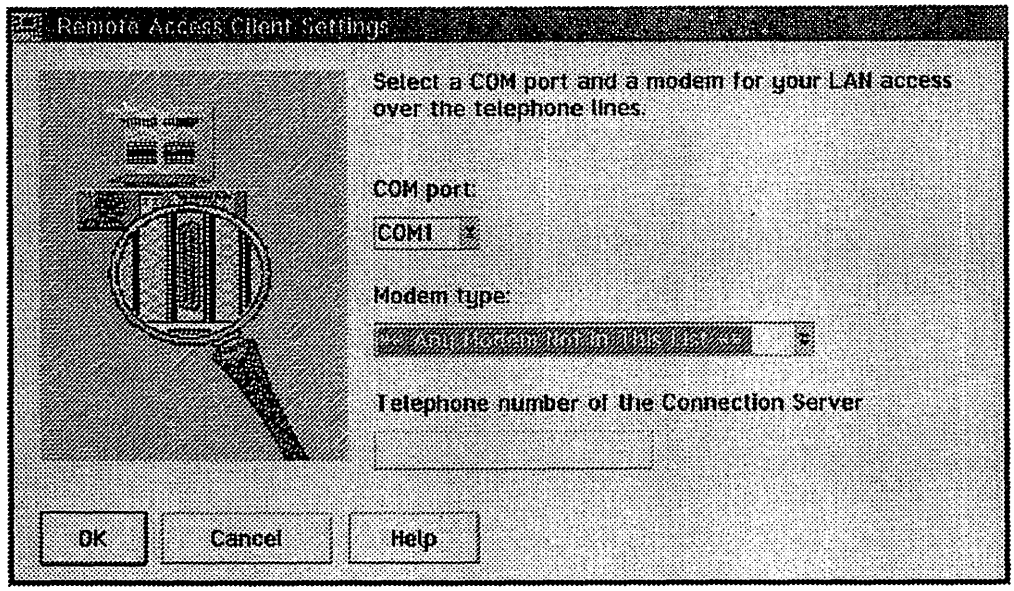


Figure 50. Remote Access Client Settings

To configure the remote access client you simply need to specify the communications port that you will be using for remote LAN connections, the type of modem that will be attached to this communications port and the telephone number that needs to be dialed to establish a connection with the connection server. For more detailed information please refer to Chapter 7, "Remote Access Services" on page 281.

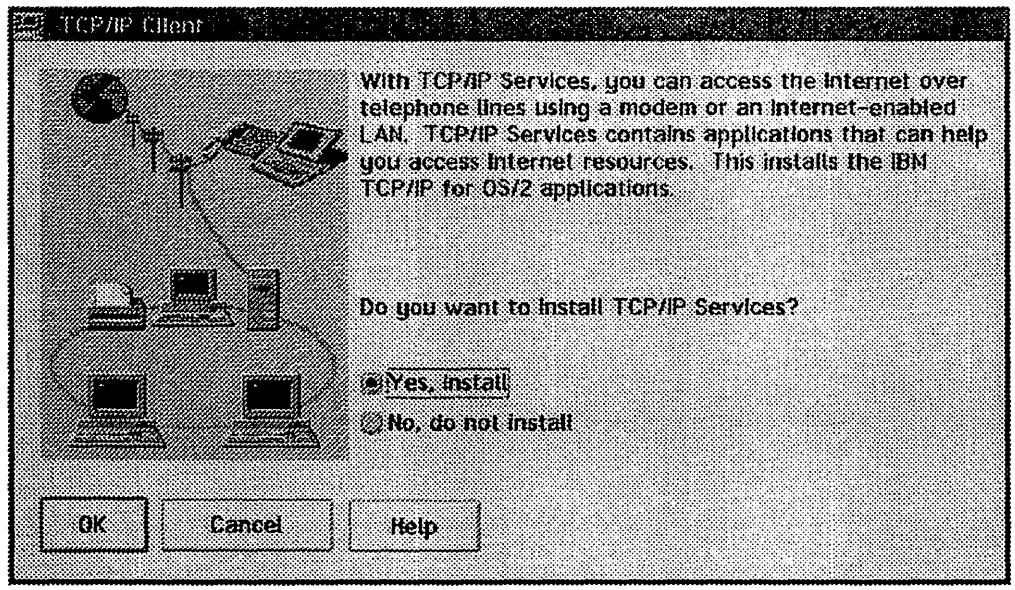

TCP/IP Client
With TCP/IP Services, you can access the Internet over telephone lines using a modem or an Internet-enabled LAN. TCP/IP Services contains applications that can help you access Internet resources. This installs the IBM TCP/IP for OS/2 applications.
Do you want to install TCP/IP Services?
Yes, install
No, do not install
OK
Cancel
Help

Figure 51. TCP/IP Client Installation

You may then specify whether you wish to install the TCP/IP client. Refer to Chapter 5, "TCP/IP Services" on page 167 for information on precisely what functions are provided.

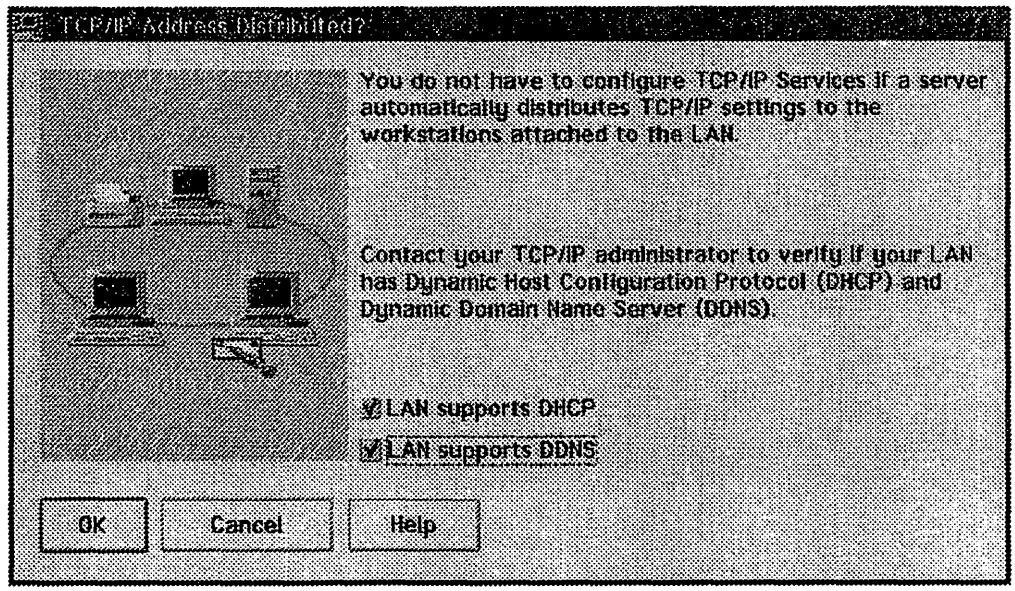

TCP/IP Address Distributed?
You do not have to configure TCP/IP Services if a server automatically distributes TCP/IP settings to the workstations attached to the LAN.
Contact your TCP/IP administrator to verify if your LAN has Dynamic Host Configuration Protocol (DHCP) and Dynamic Domain Name Server (DDNS).
LAN supports DHCP
LAN supports DDNS
OK
Cancel
Help

Figure 52. TCP/IP Client Installation - DHCP/DDNS Support

You will find a definition and an explanation of both the Dynamic Host Configuration Protocol (DHCP) and Dynamic Domain Name Server (DDNS) in Chapter 5, "TCP/IP Services" on page 167.

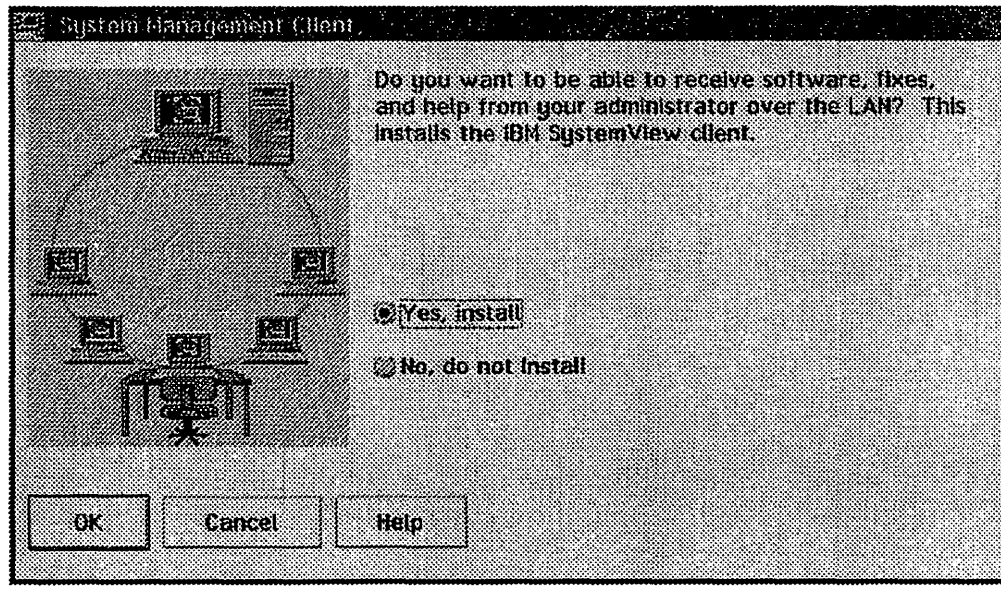

System Management Client
Do you want to be able to receive software, fixes, and help from your administrator over the LAN? This installs the IBM SystemView client.
Yes, install
No, do not install
OK
Cancel
Help

Figure 53. System Management Client Installation

Finally you have the option of installing the System Management client. Systems Management Services is not discussed in this publication. A separate redbook *Inside OS/2 Warp Server, Volume 2: Using SystemView, Backup/Recovery and Advanced Print* is planned to be available in May 1996.

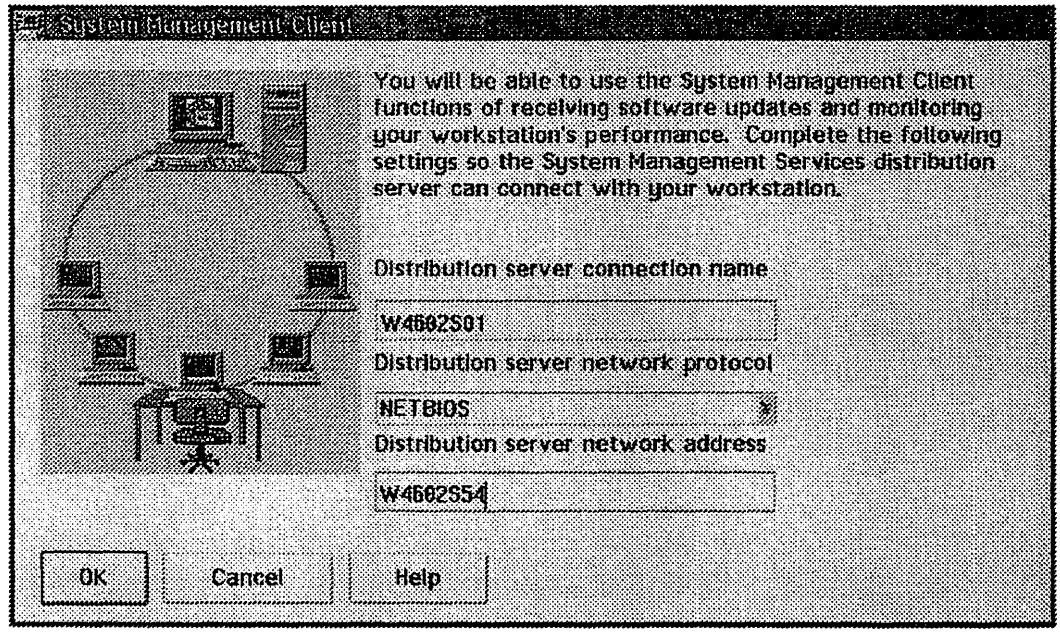

System Management Client
You will be able to use the System Management Client functions of receiving software updates and monitoring your workstation's performance. Complete the following settings so the System Management Services distribution server can connect with your workstation.
Distribution server connection name
W4602S01
Distribution server network protocol
NETBIOS
Distribution server network address
W4602S54
OK
Cancel
Help

Figure 54. System Management Client Configuration

If you select to install the System Management Client you will need to provide details of the software distribution server's address, and so on. This information will be found on the server in the General page of the SystemView Configuration panel, as shown in Figure 55.

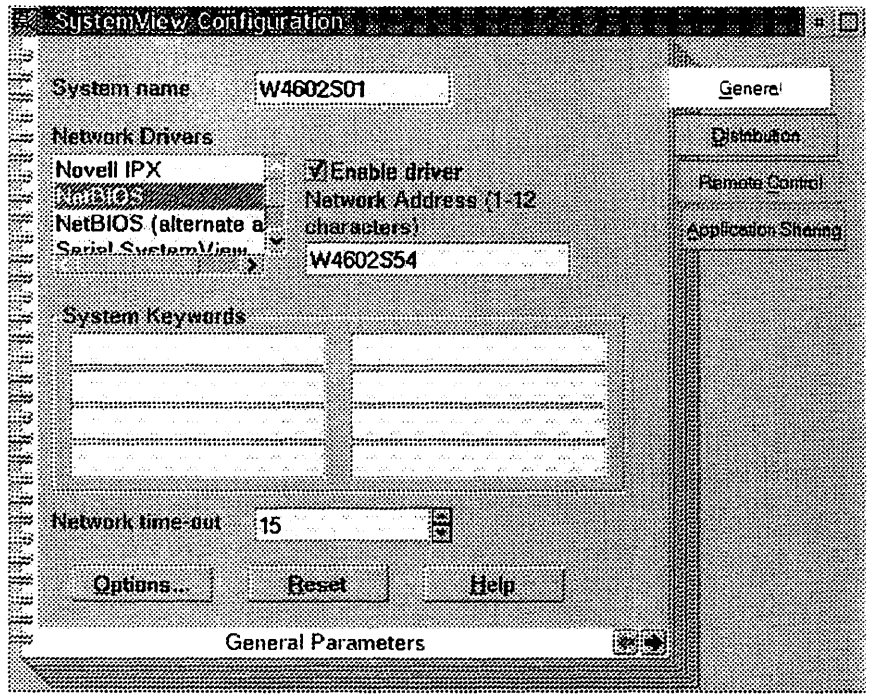


Figure 55. SystemView Software Distribution Configuration

If, in retrospect, you decide that you do want the System Management Client installed, you may remove it be performing the following steps:

1. Open the **System Management - SystemView** icon on the Desktop.

2. Open the **Install Utility** icon.
3. From the Actions menu, select **Delete**.

From CD-ROM: If you have a CD-ROM attached to the client workstation, and a version of OS/2 that is supported by OS/2 Warp Server, you may install the OS/2 client components by inserting the OS/2 Warp Server CD-ROM and typing the following with the CD-ROM as the current drive `d:`

```
d:\OS2\CLIENT\INSTALL
```

The remainder of the procedure is very similar to the remote installation method.

Cancelling Local Client Installation

To cancel the installation before it begins, just select **Cancel** on the following Workplace Shell message:

```
Are you sure you want to close all windows and active programs...
```

Then type the following command at an OS/2 command prompt:

```
c:\OS2CLNT\CLIENTS\CASCLEAN d:
```

where `c:` is the drive you selected for the installation subdirectory and `d:` is the OS/2 system boot drive.

OS/2 Client Installation Considerations

Serviceability and Diagnostic Aids

OS/2 Warp Server Remote Client requires the Serviceability and Diagnostic Aids of OS/2 Warp be installed. Do not deselect this OS/2 Warp install option. The following messages might be displayed at reboot if you deselect this option:

```
(SYS1718) The System cannot find the file  C:\OS2\LOG.SYS
(SYS1718) The System cannot find the file  C:\OS2\MDOS\LPTDD.SYS
(SYS1718) The System cannot find the file  C:\OS2\SYSTEM\LOGDAEM.EXE
```

Incomplete Client Installation Caused by PCMCIA Drivers

Before installing OS/2 Warp Server client software over an existing version of OS/2 Warp on a PCMCIA workstation, edit the workstation's CONFIG.SYS file and remove or comment out lines that contain any of the following driver names:

- PCM2ATA.SYS
- ICMEMMTD.SYS
- ICMEMCDD.SYS

To comment out a line in the CONFIG.SYS file, add the keyword REM to the beginning of the line. Save the changed CONFIG.SYS file; then shut down and restart the workstation.

If any of these drivers are present, the file and print sharing client installation program can fail.

Client LAN Adapters

For more information on installing specific adapter cards, see the READMAC.TXT file located in the \CID\NIFS directory on CD-ROM 1. If you encounter a problem, you may need to contact the manufacturer of your adapter card for technical support.

Installing Clients With No LAN Adapter

Select **NO ADAPTER** from the adapter driver list. This selection will install the IBM Parallel Port adapter on your workstation, and will allow you to install any combination of OS/2 Warp Server Remote Client products. At startup time you will see the following message:

```
The IBM Parallel Port ANDIS MAC Driver is installed.
```

Without a LAN Adapter you are limited in the connectivity functions that you can perform; however, you can use the TCP/IP async connection (SLIP or PPP) to connect to other TCP/IP systems or you can use LAN Distance Remote to connect over an async modem to a LAN Distance Connection Server and use IBM Peer for OS/2 or IBM LAN Requester to access a LAN.

If you subsequently need to add an adapter, you may do so by performing the following steps:

1. Shut down and turn off your workstation.
2. Install the new LAN Adapter.
3. Turn on your workstation.

   Note: If you have installed LAN Distance Remote, you must remove it before continuing. You can use the LDREMOVE command, located in the \WAL directory, to remove LAN Distance Remote.
4. In the OS/2 System folder, open **System Setup**; then open the **Adapters and Protocol Services MPTS** object.

   Note: You alternatively might issue the following command from an OS/2 command line: \IBMCOM\MPTS.
5. Select **Configure**.
6. In the Configure window, select **LAN Adapters and Protocols**; then select **Configure**.
7. In the Current Configuration area of the LAPS Configuration window, select **IBM OS/2 NETBIOS** under **IBM Parallel Port** in the list.
8. Select **Remove**; then select **Yes** in the confirmation window.
9. The IBM Parallel Port is now highlighted. Select **Remove**; then select **Yes** in the confirmation window.
10. In the Network Adapters area, select the adapter type you installed; then select **Add**.
11. In the Protocols area, select **IBM OS/2 NETBIOS**; then select **Add**.
12. Select **OK**.
13. Select **Close** in the Configure window; then select **Exit** to close MPTS.
14. Shut down and restart your workstation.

Installing OS/2 Client on ThinkPad

If you are installing OS/2 on an IBM PS/2 Model 76 or an IBM ThinkPad 700, 700C, 720, or 720C, you need to replace the ABIOS files on the OS/2 Installation diskette with files from the Reference diskette. Do the following:

1. If you are using a ThinkPad, detach it from the docking station. Create a Reference diskette by following the documentation that came with your computer.
2. Make a copy of the Installation diskette. Type the following command and press Enter:

   ```
   DISKCOPY A: A:
   ```

   Remove and insert diskettes when prompted to do so.
3. Remove the copy from drive A: and insert the original Installation diskette.
4. Turn your computer on. If your computer is already on, press Ctrl + Alt + Del to restart it.
5. When you are prompted to do so, remove the Installation diskette, insert diskette 1, and press Enter.
6. When the Welcome screen is displayed, press F3 to display the command prompt.
7. Insert the copy of the Installation diskette into drive A:.
8. Type `A:\DEL *.BIO` and press Enter.
9. Remove the copy of the Installation diskette and insert the Reference diskette you created into drive A:.
10. If your computer has more than one diskette drive, insert the copy of the Installation Diskette into drive B:. In the next two steps, you will be prompted to insert diskettes into both drive A: and drive B:. If your computer has only one diskette drive, when you are asked to insert a diskette into drive A:, insert the Reference diskette into the diskette drive. When you are asked to insert a diskette into drive B:, insert the copy of the Installation diskette into your diskette drive.
11. Type `COPY A:\*.BIO B:\` and press Enter.
12. Type `COPY A:\ABIOS.SYS B:\` and press Enter.
13. Turn off your computer.
14. If you are using a ThinkPad, return it to the docking station.

The OS/2 Warp Server Remote Client does not automatically detect the ThinkPad 755CD adapter type. You must select the PCMCIA option during installation.

The IBM ThinkPad 755CD's default audio configuration of Memory IO = X'220' can conflict with many PCMCIA (credit card) LAN cards. The PCMCIA cards' Memory IO = X'A20' so the conflict with the X'220' sound feature is not obvious. However, the sound feature is an emulation of the Sound Blaster 16 card which only has 10 bit addressing, and the last 10 bits of both the PCMCIA and Sound Blaster 16 cards are the same '10 0010 0000' in binary.

To install a PCMCIA Token Ring or a PCMCIA Ethernet card into an IBM ThinkPad 755CD you must change the audio Memory IO address to X'240' (or some other unused address).

If you have conflicting IRQs or Memory IO addresses you will see an error flashed on the screen for 10 seconds during restart that says the IBM2SS01.SYS file did not load.

Then you receive a restart message that your LAN device driver did not load.

PCMCIA Token-Ring cards and the Future Domain SCSI adapter can interact to cause I/O errors on a CD-ROM attached to the SCSI adapter. To avoid these I/O errors, change the SCSI Controller Memory Address on the Docking Station I from CA00 to an unused memory address (CE00 or DE00). Refer to the IBM ThinkPad Dock I Users Guide (part number 71G4054) page 5-5 for instructions on how to change the SCSI Controller Memory Address.

The 701 ThinkPad Chips and Technology Video comes set to MMIO=CC00. This conflicts with the MMIO default on several PCMCIA cards. Reset the MMIO on the 701 video to D400 to avoid conflicts with PCMCIA cards. The 701 audio can also conflict with the IRQ and IOAddress of the PCMCIA cards. To get started you can disable the audio function, install OS/2 Warp Server Remote Client, then enable the audio at addresses and IRQs that are not used by the PCMCIA cards.

ThinkPads on Dock II docking stations with Adaptec SCSI adapters can hang during OS/2 Warp Server Remote Client install. To prevent this hang, change the SCSI port address from 340h to 140h using the switch block switch number 4. Page 78-79 of the IBM ThinkPad Dock II User's Guide (part number 84G9682) describes where the switch block is located and how to change the port address of the SCSI adapter.

Graphical User Interface

As discussed in 2.6, "Sharing Resources with the Administration GUI" on page 19, you can access the OS/2 Warp Server Administration GUI, as shown in Figure 56 on page 61, from the IBM LAN Services folder or from the Network folder.

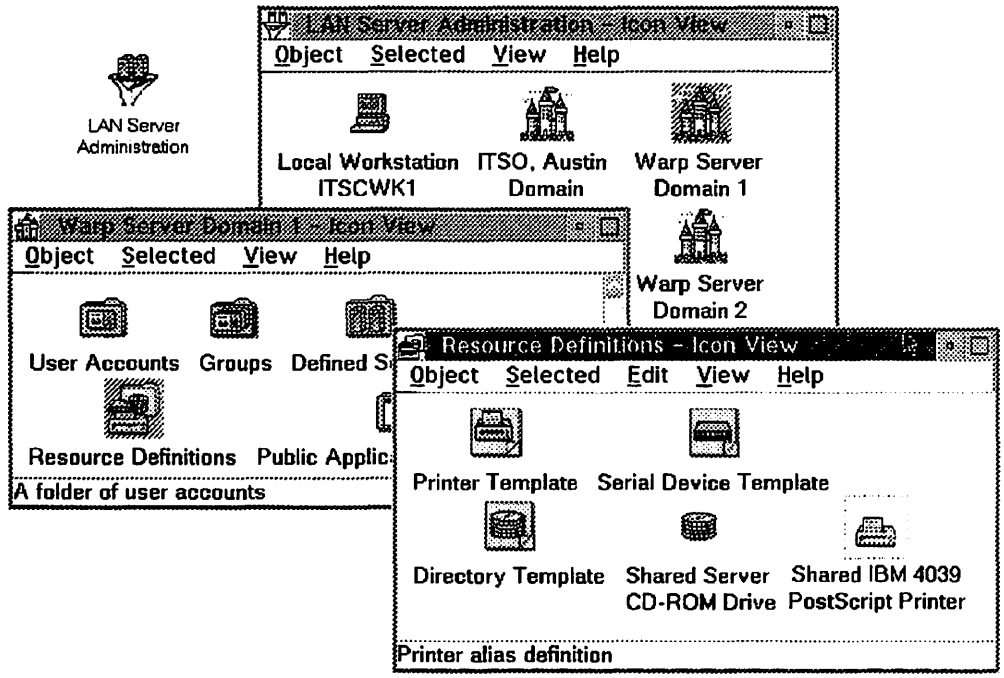


Figure 56. OS/2 Warp Server Administration Graphical User Interface

If you are logged on as a user without administrator privileges then you will only be able to modify changes to your user account definition, such as your password and logon assignments, as shown in Figure 57 on page 62.

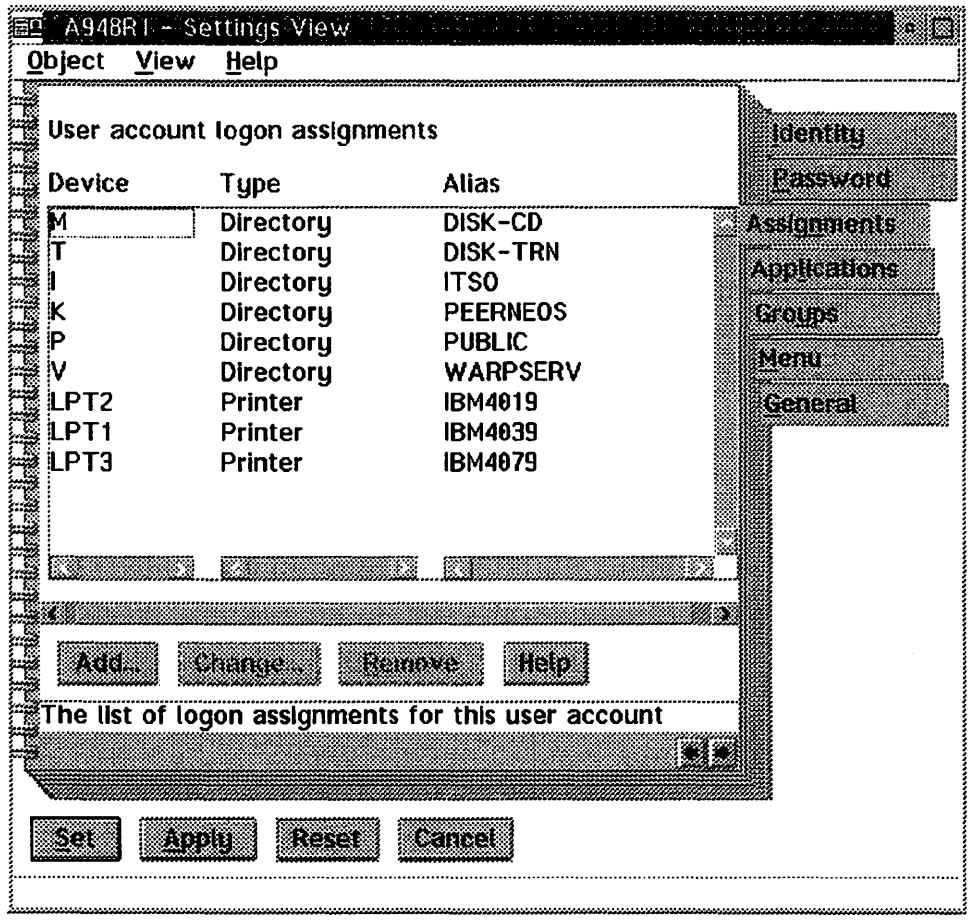


Figure 57. Modifying your User Account Settings

Connecting to Network Resources from the OS/2 File and Print Client

After the administrator of the domain has defined a resource as an alias and granted you permission to access it, a local device name needs to be assigned to the alias before you can use it.

A local device name is a drive, LPT port, or COM port defined on your workstation. The type of resource you are using (directory, printer, or serial device) determines the local device name you should use.

Local device names for directories and files are drive letters. Local device names for printers are printer ports (LPT1, LPT2, and so on). Serial devices (modems and plotters) may be addressed as either LPT ports or COM ports.

The Network Resource Browser (found in the Network folder, which is located in the OS/2 System folder) and the OS/2 Warp Server Administration GUI enables you to easily assign local device names to network resources. You can create two types of assignments:

- ***Logon Assignments:*** Once defined, logon assignments provide you with access to shared resources each time you logon. Figure 58 on page 63 shows how you add a logon assignment for an additional directory resource.

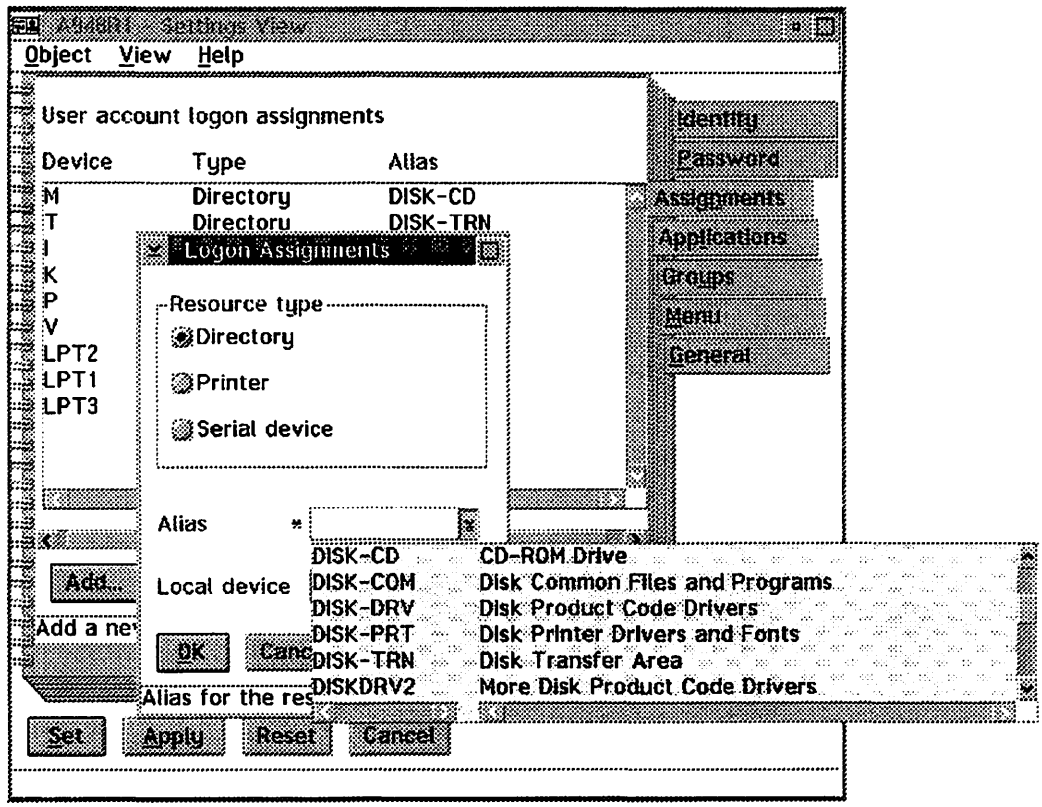


Figure 58. Adding Logon Assignments

- ***Current Assignments:*** Similar to logon assignments except that the assignments will only remain active for the current session and will be lost when the user logs off. Figure 59 on page 64 shows how you define a temporary current assignment.

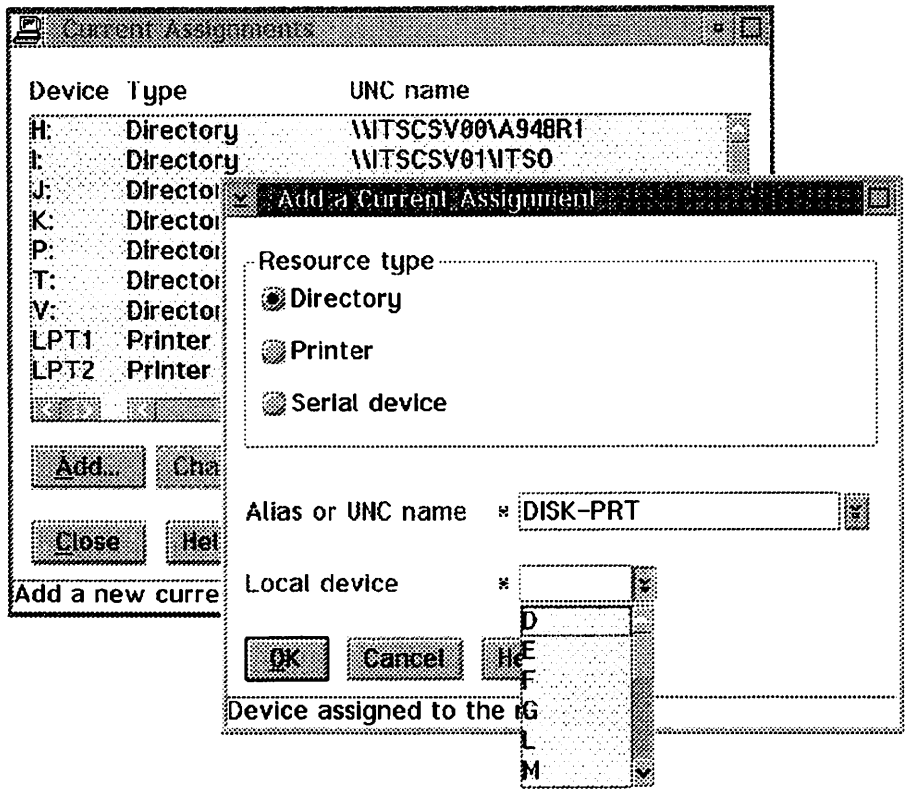


Figure 59. Adding Current Assignments

This window is accessed by selecting your local workstation object with mouse button 2 from the initial window that is displayed when you start the OS/2 Warp Server Administration GUI and selecting **Current Assignments**.

3.3 DOS File and Print Client (DOS LAN Services)

DOS LAN Services is the component of OS/2 Warp Server that provides LAN connectivity for users of workstations running DOS and features some significant enhancements to the original version of DOS LAN Services provided with OS/2 LAN Server 4.0.

DOS LAN Services may function in a DOS environment with or without Windows. In a pure DOS environment, a graphical user interface with pull down menus is provided.

In addition, the more experienced user or LAN administrator may perform network tasks or automate repetitive functions via `NET` commands from the DOS command line or via DOS batch files. Using `NET ADMIN`, an administrator at a DOS LAN Services workstation can manage servers remotely using the command line interface.

The main features and functions of DOS LAN Services are:

- DOS Graphical User Interface
- Access to network resources
- Network messaging
- Peer Services (client single-connection resource sharing)

- Network DDE/Clipboard (for Windows)
- Reduced memory requirements
- Automatic session/optional *persistent connection* reconnection
- LAN API support

The following functional restrictions apply, such that DOS LAN Services cannot:

- Use shared serial devices unless a serial printer is defined at the server as a shared parallel printer
- Start from the DOS Shell
- Perform remote administration of a server workstation from the GUI
- Be installed if the DOS PATH statement would exceed 127 characters after adding the path for the DOS LAN Services code (DOS restriction)
- Run when the DOS Shell is loaded
- Run in an OS/2 emulated DOS session (VDM)
- Change connections from a domain controller to a backup domain controller if the former fails

The specific functions of each individual DOS LAN Services module are detailed in Table 10 on page 104.

New Features

DOS LAN Services was introduced with OS/2 LAN Server 4.0 and included a number of significant enhancements to the DOS LAN Requester shipped with previous versions of LAN Server.

In OS/2 Warp Server, DOS LAN Services has been further enhanced with the following features:

- Conservation of conventional memory (see "Reduced Memory Requirements" on page 77)
- Remote installation enhancements (see "Remote Installation (CID)" on page 74)
- Integrated TCPBEUI installation (see 3.12, "DOS LAN Services Common Configuration Scenarios" on page 105)
- Support for Windows 95 (see 3.5, "Windows 95 Client (DOS LAN Services for Windows 95)" on page 87)
- User Level Security for the Peer Service (see "User Level Security" on page 98)
- Improved integration on OS/2 workstations (see 3.6, "Installing and Running DOS LAN Services on OS/2" on page 91)
- Windows GUI Customization Options (see "Customizing your DOS LAN Services Windows GUI" on page 83)
- Network drive conservation (see "DOS LAN Services Windows Shared Applications" on page 86)

Installation

Before you can set up DOS LAN Services, make sure that a network adapter is installed in your workstation and that the adapter is connected to a network.

To install a network adapter and configure it:

1. Verify that you have the required hardware, such as the network adapter, cables, connectors, and other items you will need during installation.
2. Configure your network adapter so that it will work with your workstation. Some adapters must be configured before you install them. Others must be configured after you install them.
3. Install the network adapter in your workstation.
4. Connect the cables to the network adapter and to the other workstations in your network.

For information about how to install your network adapter, see the documentation that came with the adapter.

Previously, just to install DOS LAN Services, that was packaged with OS/2 LAN Server 4.0, you required approximately 500KB of conventional memory. A protected mode installer, capable of addressing more than 1MB of memory, has been added to the DOS LAN Services code that is included with OS/2 Warp Server. This significantly reduces the amount of conventional memory that you need to have available before you can install DOS LAN Services on systems with 80286 processors or higher.

To install DOS LAN Services, the following software is required:

- DOS 3.3, DOS 5.02 or higher
- OS/2 Warp Server Entry or OS/2 Warp Server
- Microsoft Windows 3.1 (optional)

  Note: Microsoft Windows 3.0 is not supported by DOS LAN Services because the DOS LAN Services code base is dependent upon certain Windows 3.1 APIs.

There are a number of methods that you may use to install DOS LAN Services.

Installation from Diskette

You may create DOS LAN Services installation diskettes from images stored on the OS/2 Warp Server CD-ROM. You will require four formatted diskettes which you should label DOS LAN Services Diskette 1 to 4 inclusive. You then simply copy the contents of the following directories onto each of the four diskettes:

```
d:\CID\SERVER\IBMLS\IBM500D1 (DOS LAN Services Diskette 1)
d:\CID\SERVER\IBMLS\IBM500D2 (DOS LAN Services Diskette 2)
d:\CID\SERVER\IBMLS\IBM500D3 (DOS LAN Services Diskette 3)
d:\CID\SERVER\IBMLS\IBM500D4 (DOS LAN Services Diskette 4)
```

where `d` is the CD-ROM drive letter.

If you need to install additional protocol support then you may also create a LAN Support Program Diskette (`d:\CID\SERVER\IBMLS\IBM500L1`).

After you have created the DOS LAN Services product diskettes you may then install DOS LAN Services by inserting diskette 1 in the workstation's diskette drive and typing:

```
a:\INSTALL
```

where a is the diskette drive letter.

Installation Switches

One of the optional parameters (/I), that may be used with the INSTALL command, disables network adapter hardware detection. Use this option only if INSTALL will not run without it. If you use this option, you must specify your hardware configuration during the installation process.

Note: DOS LAN Services does not include drivers for PCMCIA network adapters therefore you should install support for these adapters before installing DOS LAN Services with the /I switch.

A new switch (/N) has been added to the INSTALL command. Use this option if your adapter and associated LAN transport components are already configured and you want to install the services provided by DOS LAN Services without changing the adapter/transport configuration.

Additional parameters may be passed to INSTALL.BAT to aid remote installation. These are documented in "Remote Installation (CID)" on page 74.

Default installation options are shown in Table 1 and Table 2.

Table 1. DOS LAN Services Installation Options Screen 1

Installation Option	Default Setting
Graphical User Interface	Install GUI
Peer Services	Install Peer Services
Windows Support	Install Windows Support
Protocol Driver	IBM NetBEUI

Table 2. DOS LAN Services Installation Options Screen 2

Installation Option	Default Setting
Machine ID	Must be entered by user (15 characters or less)
User name	Must be entered by user (20 characters or less)
Domain name	Must be entered by user (15 characters or less)
Redirector	Use the full redirector
Startup option	Run DOS LAN Services and log on
Path	C:\NET
Network card	Automatically detected by DOS LAN Services

For a detailed explanation of each option, refer to *Network Administrator Reference Volume 1: Planning, Installation and Configuration* which is shipped with OS/2 Warp Server as an installable online book.

Note: If you reinstall Windows or modify the DOS LAN Services configuration file (NETWORK.INI) you must run the DOS LAN Services install program (INSTALL.BAT). Also note that DOS LAN Services cannot be run from the DOS shell. Therefore, you should either remove the DOSSHELL statement from your AUTOEXEC.BAT or move it to run after the DOS LAN Services statements.

While referring to this section for additional guidance, follow the installation instructions displayed on the screen and select the options that best suit your requirements.

If you experience any problems installing DOS LAN Services then you will find hints and tips in the file CONNECT.TXT in the directory where DOS LAN Services was installed.

Installation from the OS/2 Warp Server CD-ROM

Alternatively, if you have a CD-ROM attached to your DOS/Windows workstation you may install DOS LAN Services by typing:

```
d:\DOS\CLIENT\INSTALL
```

where d is the CD-ROM drive letter.

The installation procedure then follows the same flow as if you were remotely installing from an OS/2 Warp Server server, as described in "Remote Installation (from an OS/2 Warp Server)," but without the steps necessary to establish a remote connection.

Remote Installation (from an OS/2 Warp Server)

As is the case with the OS/2 file and print client, you may remotely install the DOS/Windows file and print client across the LAN from images stored on the server workstation's hard drive or CD-ROM. You can do this by generating a DOS Remote Installation Diskette by following the procedure detailed in 2.8, "Preparing the Server for Client Installation" on page 28 and select Windows workstation on the screen shown in Figure 28 on page 29.

Remote Installation Prerequisites

To perform a remote installation of a Windows workstation you *must* have DOS and Windows 3.1 or Windows for WorkGroups already installed.

After generating your DOS Remote Installation Diskette you simply take it to your LAN attached DOS/Windows workstation and type:

```
a:\INSTALL
```

where a is the diskette drive letter.

Note: If your system appears to hang please verify that when you created the DOS Remote Installation Diskette you selected the correct network adapter.

The OS/2 Warp Server installation program will then copy files required for the remote installation to the C:\WSINST directory on the workstation and, depending on the current workstation configuration, you may need to select the option to install the remote connection support unless you are running one of the following:

- PC LAN Support Program Version 1.3 or later
- DOS LAN Requester Version 2.0 or later
- DOS LAN Services Version 4.0 or later
- Microsoft LAN Manager 2.x DOS Client
- Microsoft Windows for WorkGroups Version 3.11

If you are running one of the above on your workstation then you must ensure that the network software is started before beginning the OS/2 Warp Server Windows client installation.

If not, then you need to install the remote connection support which will modify your system configuration and automatically restart the workstation. After the system restarts you may continue the remote installation by starting Windows and selecting the Windows Client Installation program icon from the WS Remote Installation program group.

Note: The remote connection support is provided by a subset of DOS LAN Services.

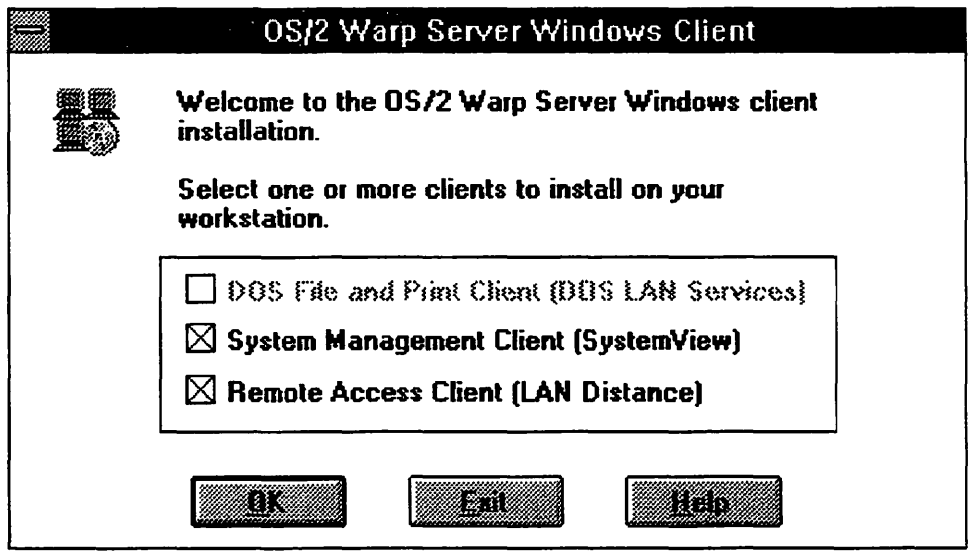

OS/2 Warp Server Windows Client
Welcome to the OS/2 Warp Server Windows client installation.
Select one or more clients to install on your workstation.
DOS File and Print Client (DOS LAN Services)
System Management Client (SystemView)
Remote Access Client (LAN Distance)
OK
Exit
Help

Figure 60. Windows Client Remote Installation - Client Selection

After the remote installation files have been copied over when you next start Windows you will be presented with the screen shown in Figure 60.

Note: In this example the target workstation already had the DOS File and Print Client installed and therefore was not selectable.

After specifying the client components that you wish to install you will then be ready to begin the installation process. In this instance the first client component that you are prompted to install is the SystemView Windows client.

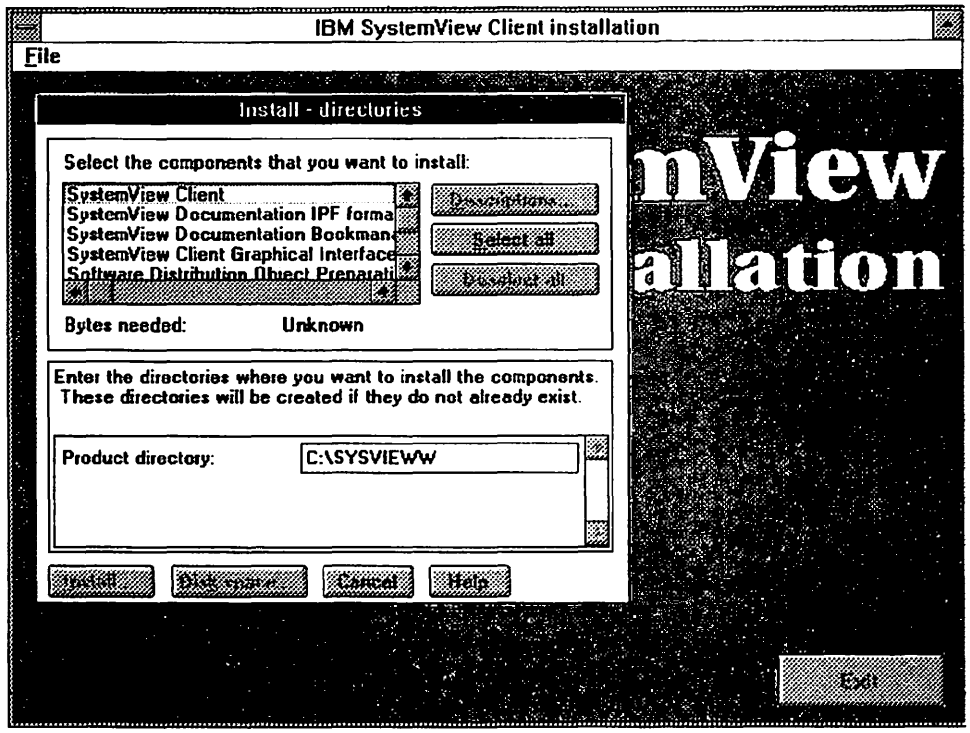


Figure 61. SystemView Windows Client Installation

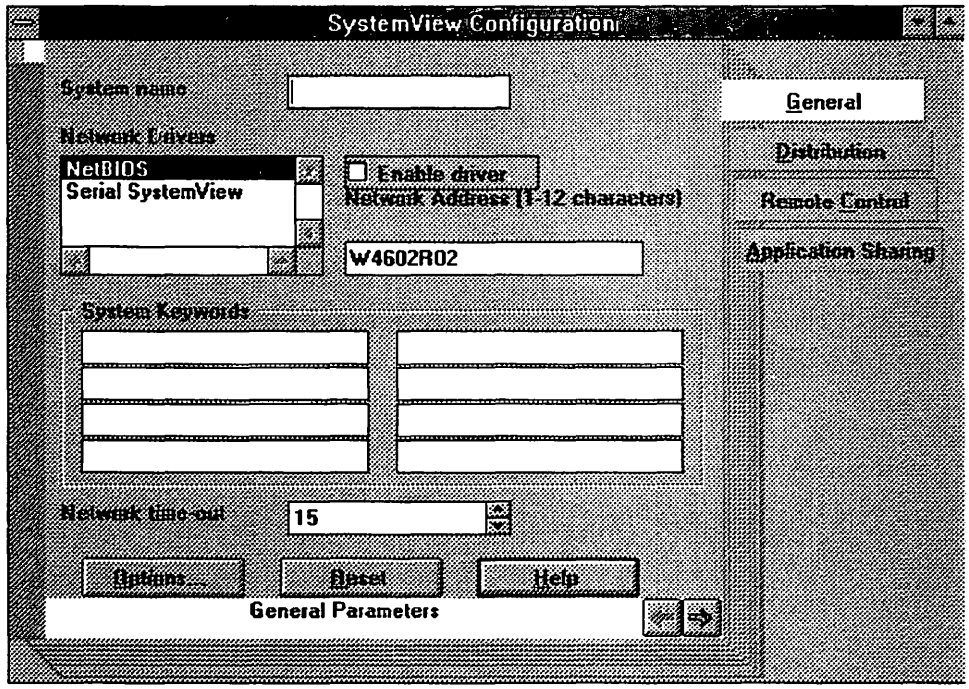


Figure 62. SystemView Windows Client Configuration

Figure 61 and Figure 62 show what you are presented with when you select the SystemView for Windows client and Figure 63 on page 71 shows the resulting program group after installation. For a detailed discussion of the SystemView for Windows components please refer to *Inside OS/2 Warp Server, Volume 2: Using*

SystemView, Backup/Recovery and Advanced Print which is planned to be available in May 1996.

Note: If the following message is received during the OS/2 Warp Server Windows Client installation:

```
"STOP" It was not possible to write the distribution configuration
due to TCP/IP (or NetBIOS) Problems.
```

Select **Cancel**. After you complete the installation, open the SystemView icon and re-configure these protocols.

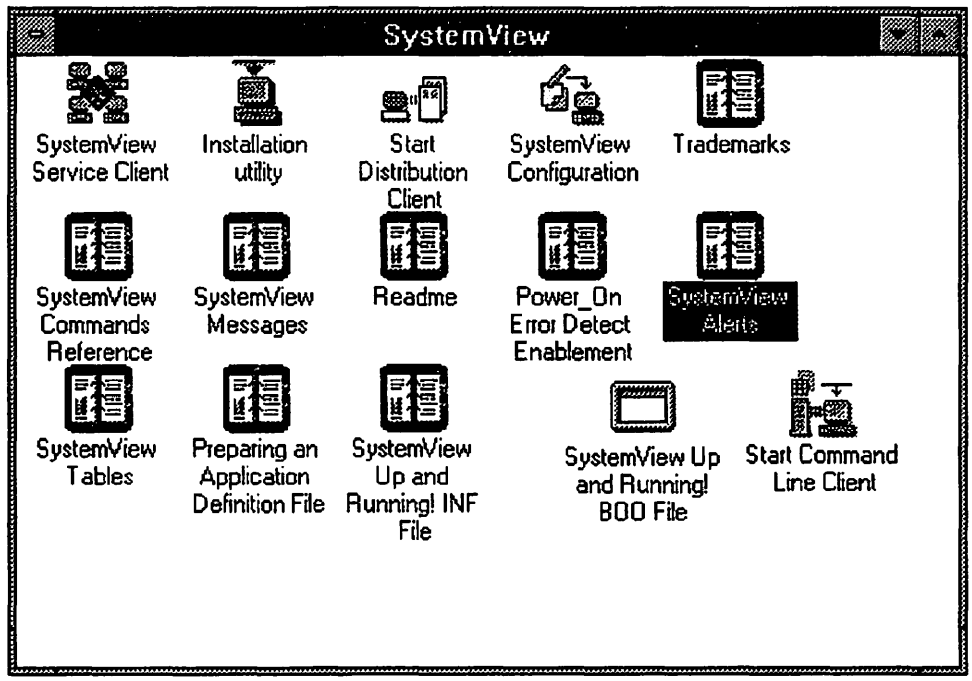


Figure 63. SystemView for Windows Program Group

After the SystemView client is configured and installed you are then automatically prompted to configure and install the Remote Access client. Figure 64 on page 72 through Figure 69 on page 74 show some of the screens that guide you through the Windows Remote Access client installation. For a detailed discussion please refer to 7.6, "Setting Up a Windows Remote Access Services Client" on page 317.

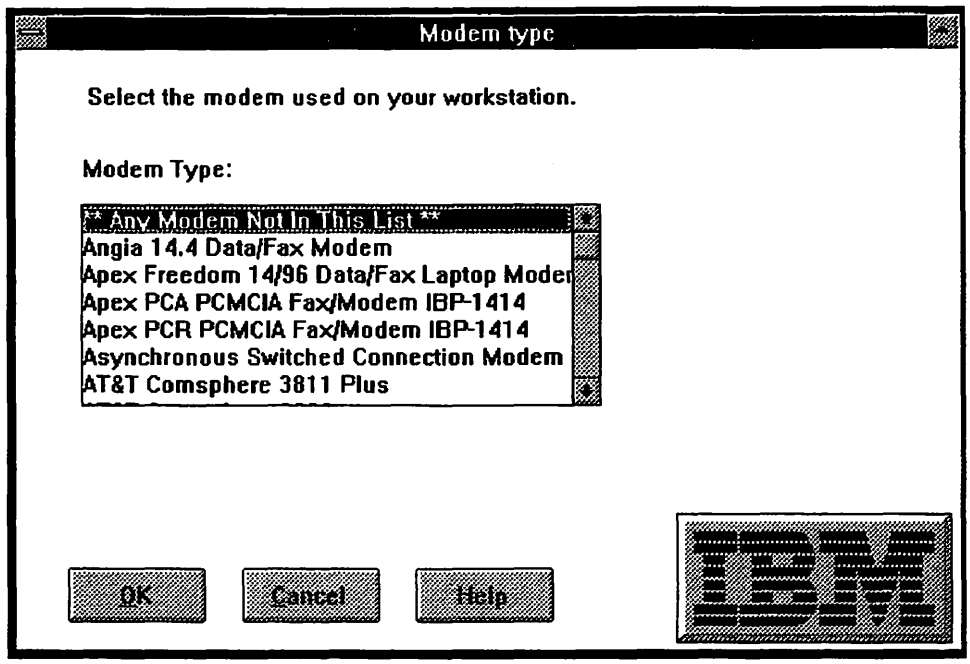


Figure 64. Windows Remote Access Client - Select Modem Type

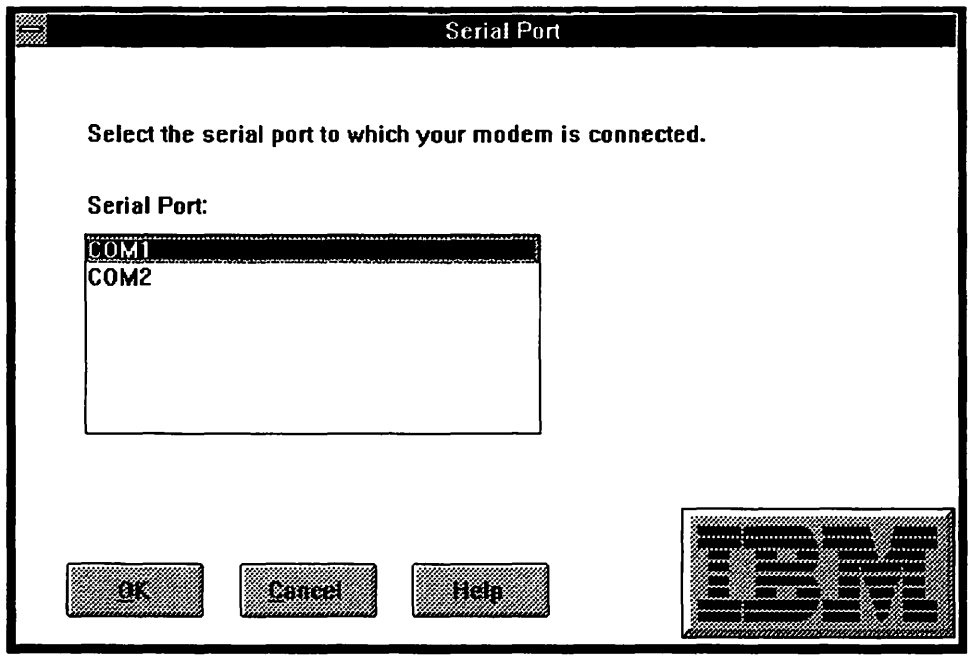


Figure 65. Windows Remote Access Client - Specify Serial Port

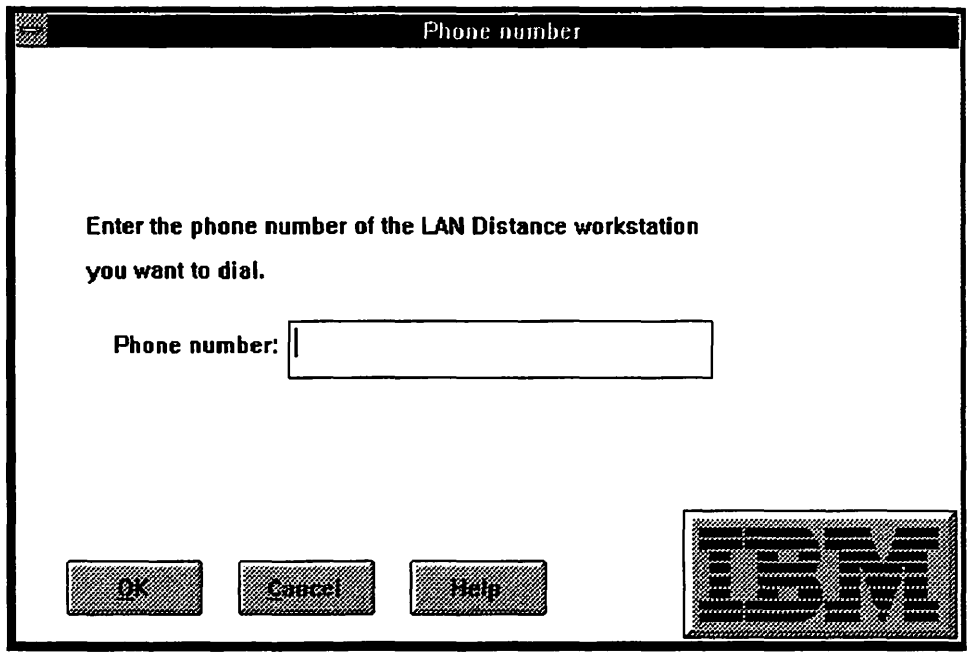


Figure 66. Windows Remote Access Client - Specify Phone Number

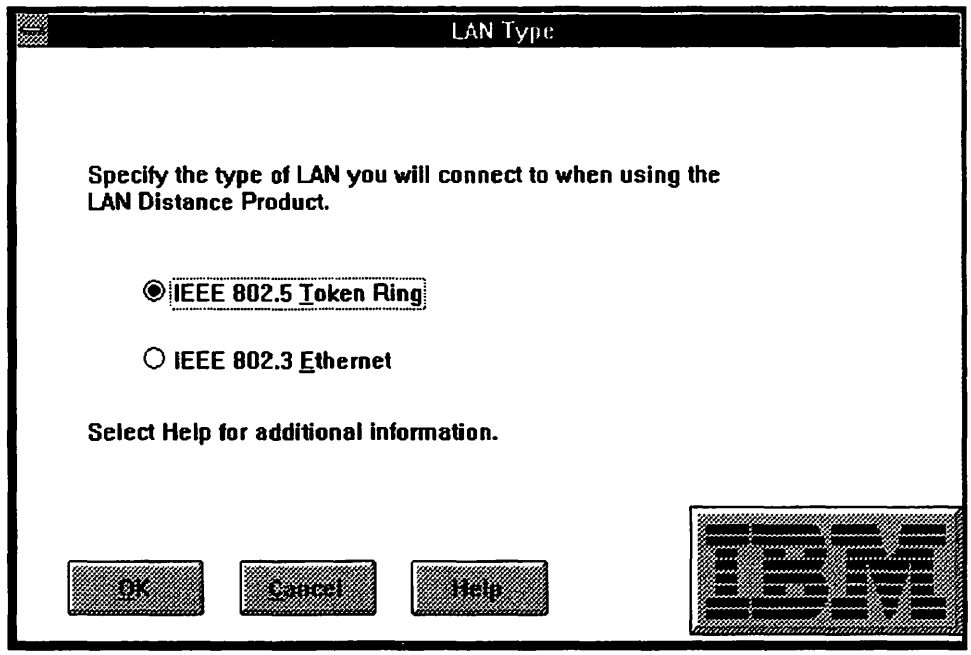


Figure 67. Windows Remote Access Client - Select LAN Type

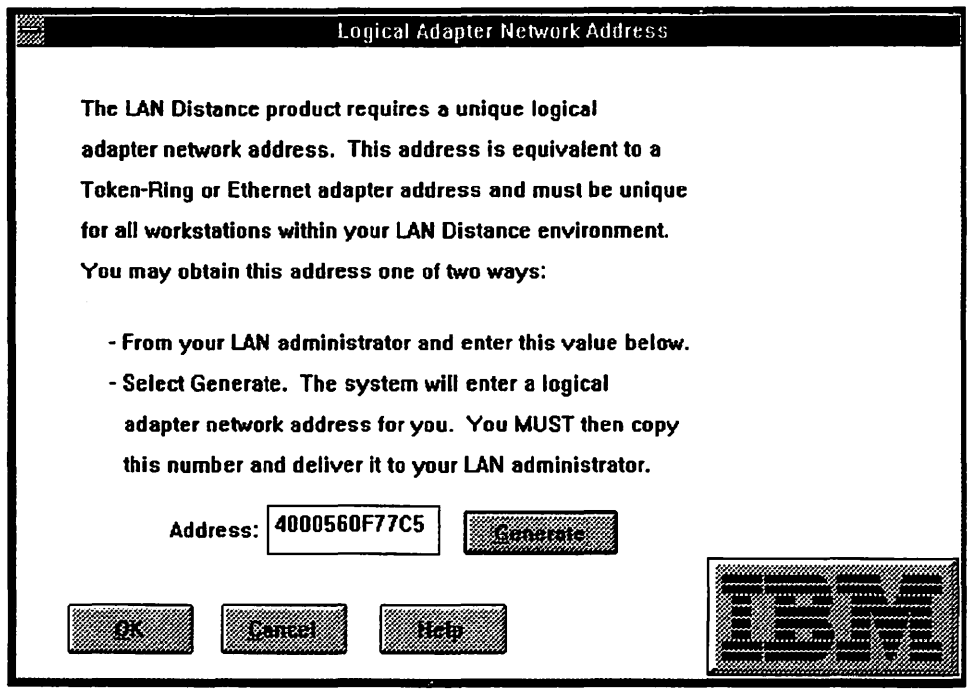

Logical Adapter Network Address
The LAN Distance product requires a unique logical adapter network address. This address is equivalent to a Token-Ring or Ethernet adapter address and must be unique for all workstations within your LAN Distance environment. You may obtain this address one of two ways:
- From your LAN administrator and enter this value below.
- Select Generate. The system will enter a logical adapter network address for you. You MUST then copy this number and deliver it to your LAN administrator.
Address:
4000560F77C5
Generate
OK
Cancel
Help

Figure 68. Windows Remote Access Client - Generate Logical Adapter Address

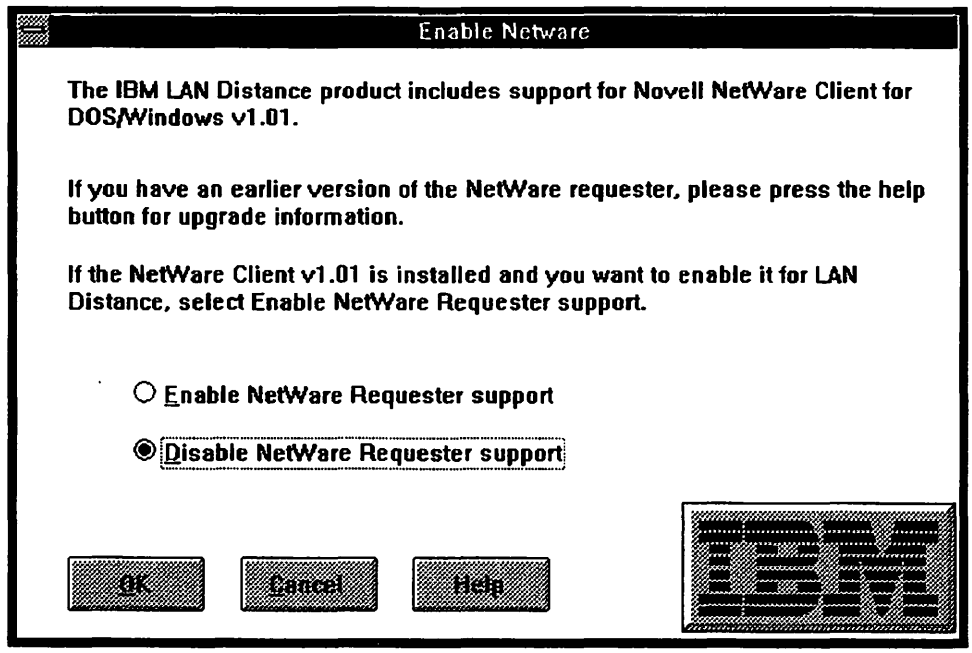

Enable Netware
The IBM LAN Distance product includes support for Novell NetWare Client for DOS/Windows v1.01.
If you have an earlier version of the NetWare requester, please press the help button for upgrade information.
If the NetWare Client v1.01 is installed and you want to enable it for LAN Distance, select Enable NetWare Requester support.
Enable NetWare Requester support
Disable NetWare Requester support
OK
Cancel
Help

Figure 69. Windows Remote Access Client - Enable NetWare Support

Remote Installation (CID)

DOS LAN Services clients are CID-enabled to allow for attended, lightly attended and unattended installation from a code server. This is quite different from the native OS/2 Warp Server remote installation method which is discussed in "Remote Installation (from an OS/2 Warp Server)" on page 68.

Previously, in order to perform a remote installation of a system with no operating system installed, you needed to setup a SRVIFS code server and produce two remote installation boot diskettes that contained an OS/2 and SRVIFS client.

In this latest version of DOS LAN Services you may now create one remote installation boot diskette which contains DOS, the DOS LAN Services client and LAN Support Program (LSP) transport. Since DOS LAN Services uses native LAN Server protocols, it is not necessary to have SRVIFS on the code server.

To aid remote installation the following option switches have been added to the DOS LAN Services INSTALL command:

- [/L1] enables you to specify where you want the remote error log file to be stored. For example:

  ```
  INSTALL /L1:C:\DLS.ERR
  ```

- [/L2] enables you to specify where you want the remote history log file to be stored. For example:

  ```
  INSTALL /L2:C:\DLS.HIS
  ```

- [/R] is required for remote installation and specifies where the DOS LAN Services response file is stored. For example:

  ```
  INSTALL /R:C:\DLSRSP\DLS.RSP
  ```

Implementation of this new feature has also added new command line options to the NET START and NET LOGON commands in DOS LAN Services.

The new option switches for NET START are:

- [/COMPUTERNAME:{name | *}] temporarily replaces the computername parameter specified in NETWORK.INI. The asterisk (*) prompts for the automatic random generation of a temporary name for the computer.
- [/AUTOLOGON:NO] temporarily modifies the autologon behaviour of the requester. Only an override of NO is allowed.

The new option switches for NET LOGON are:

- [/LSLOGON:NO] temporarily changes the validated logon behaviour of the requester. Only an override of NO is allowed.
- [/GENID] temporarily overrides the user name specified in NETWORK.INI with an automatically randomly generated user name.
  - /GENID is mutually exclusive with a user ID and/or password specified on the command line.
  - /GENID automatically includes /PWCACHING:NO.
  - /GENID automatically surpresses prompting (/YES).
- [/PWCACHING:NO] temporarily changes the the password caching behavior as specified in NETWORK.INI. Only an override of NO is allowed.

Response File Parameter Reference: The following table provides information on the keywords that you may use in the response file for DOS LAN Services CID installation.

Table 3. DOS LAN Services Remote Installation - Response File Keyword Reference			
Keyword	**Description**	**Valid Values**	**Default**
configsys	Where CONFIG.SYS is located	A valid path	C:\
autoexecbat	Where AUTOEXEC.BAT is located	A valid path	C:\
target	Drive and directory to install DOS LAN Services	A valid path	C:\NET
peer	Switch for installing Peer support	Yes, No	No
windowsupport	Switch for installing Windows support	Yes, No	No
gui	Switch for installing GUI support	Yes, No	No
install802	Switch for installing 802.2 support. If this switch is set to Yes, LAN Support Program (non-NDIS) will be loaded.	Yes, No	No
computername	The name that identifies the workstation to the network	Up to 15 alphanumeric characters or special characters including ! # $ % & ( ) ¢ _ { } ^ ` ~	You must supply this information
domainname	The name that identifies the domain that this workstation belongs to	Up to 15 alphanumeric characters or special characters including ! # $ % & ( ) ¢ _ { } ^ ` ~	You must supply this information
username	The name that identifies you to the network	Up to 20 alphanumeric characters or special characters including ! # $ % & ( ) ¢ _ { } ^ ` ~	You must supply this information
networkcard	DOS LAN Services will try to automatically detect your network card so this parameter will, in most instances, not be needed on your system. If you specify this parameter in your response file, DOS LAN Services will install the driver for the card specified.	See *Network Administrator's Reference*	No parameter specified

Sample DOS LAN Services Response File: The following is the sample DLSNEW.RSP response file included with DOS LAN Services which may be found on DOS LAN Services Diskette 1.

```
[dlsmain]
computername=jimsmach
configsys=c:
username=jimmyp
domainname=kawasaki
autoexecbat=c:
target=d:\net
peer=yes
redirecter=full
windowsupport=yes
gui=yes

[dlsdriver]
ncbs=30
sessions=33
```

Figure 70. Sample DOS LAN Services Response File

Reduced Memory Requirements

Given the limitations imposed by DOS on real mode memory, it is obviously critical to minimize the use of it. Continuous efforts are focussed on increasing the amount of memory available for applications. The result is that on an 8086/8088-based workstation configured as a basic redirector running DOS 3.3 with LAN Support Program, 496KB of conventional memory remains available to applications. DOS LAN Services, as shipped with OS/2 Warp Server, incorporates a protected mode redirector which provides a similarly configured 386 or 486 workstation, running PC-DOS 7.0, with 621KB of real mode memory available.

Even running the protected mode redirector results in 598KB of memory available to DOS applications!

Note: The above values are based on 110KB of Upper Memory Block (UMB) space. These values represent the amount of conventional memory that is available after loading the LAN Transport and DOS LAN Services redirector.

DOS LAN Services Fixes

To get the DOS LAN Services enhancements and fixes described in this chapter for existing OS/2 LAN Server 4.0 DOS clients, contact your IBM customer service representative and ask to be sent fixes relating to APAR IC10086 or obtain OS/2 LAN Server 4.0 Service Pack IP08150 which includes the DOS LAN Services enhancements/fixes that are included in OS/2 Warp Server.

If you are in doubt as to whether you have DOS LAN Services with the protected mode redirector then check for the file CMDS16.EXE in the directory where you have DOS LAN Services installed. If you have this file then you have the protected mode redirector.

In a Windows environment, DOS LAN Services does not actually use any real mode memory when configured as a virtual redirector, since it runs as a Windows virtual device driver.

The following sample files illustrate how you may configure a system to have 636 368 bytes (621 KB) of memory available to DOS applications after loading LAN transport and DOS LAN Services, with FILES=30 and LASTDRIVE=H.

Note: In this example, LAN Support Program has been used to minimize memory utilization. For optimum performance, IBM NetBEUI is recommended (the default when you install DLS).

These sample files were taken from an IBM PS/VP with 8MB of RAM and an IBM Auto 16/4 Token Ring ISA Adapter installed. The amount UMB space available will vary depending on the hardware configuration of the system since hardware drivers are loaded into this memory area.

```
DEVICE=C:\DOS\HIMEM.SYS
DOS=HIGH,UMB
DEVICE=C:\DOS\EMM386.EXE NOEMS RAM <---See Note 1
FILES=30                <---------------See Note 2
BUFFERS=20              <---------------See Note 3
DEVICEHIGH=C:\LSP\DXMA0MOD.SYS
DEVICEHIGH=C:\LSP\DXMC0MOD.SYS
DEVICEHIGH=C:\LSP\DXMT0MOD.SYS
LASTDRIVE=H             <---------------See Note 4
STACKS=0,0              <---------------See Note 5
DEVICEHIGH=C:\NET\DLSHELP.SYS <--------See Note 6
```

Figure 71. Sample CONFIG.SYS for Maximum Memory Availability

```
@ECHO OFF
PROMPT $P$G
PROMPT C:\;C:\DOS;C:\NET;
C:\NET\NET START
```

Figure 72. Sample AUTOEXEC.BAT for Maximum Memory Availability

```
[network]
computername=DLSREQ01
lanroot=C:\NET
autologon=no
autostart=basic       <---------------See Note 7
guiconfig=0,0,1
username=USER1
domain=TESTDOM4
lslogon=yes
reconnect=yes
passwordcaching=yes
timesync=yes

[Password Lists]
USER1=C:\NET\USER1.PWL

[Domain List]
TESTDOM4=
```

Figure 73. Sample NETWORK.INI for Maximum Memory Availability

Notes:

1. Memory include and exclude parameters are omitted from the example.
2. This represents a typical value to support most environments. The implications on memory utilization of adjusting this value are negligible.
3. Buffers are loaded into upper memory, where available, and therefore there is no impact on real mode memory unless the amount of UMB space is limited.
4. Each additional drive letter consumes between 80-100 bytes, and, therefore, you should plan your network logon assignments to maximize the available memory at the workstation.
5. Setting the value of stacks to 0,0 conserves memory but may cause problems on certain systems. Reset back to the default if your system appears unstable.
6. This driver provides an interface to the redirector. It handles hooking interrupts and some initial setup work. Without this driver, DOS LAN Services will not function.
7. The basic redirector program only supports basic network functions such as connecting, disconnecting and browsing of shared resources. If additional function is required, such as the GUI or peer services capability, then you will require the full redirector. Refer to the OS/2 Warp Server *Commands and Utilities* publication (available as online documentation; resides in the LAN Services File and Print folder) for details of the restrictions on the use of the NET USE command with the basic redirector.

Selecting the Redirector

It is important to understand the differences between the types of redirectors available:

Basic Redirector: Provides all standard requester functions, such as connecting, disconnecting and browsing. It requires less memory and disk space and should therefore be used if you:

- Have a workstation with limited processing power, such as an 8086 or 8088
- Cannot use the protected mode redirector
- Have limited memory available on your workstation
- Do not wish to use *aliases* to identify resources
- Do not plan to use Windows

Full Redirector: Provides advanced network functions, such as named pipes, as well as increased performance and full API support.

Protected Mode Redirector: Provides the same level of functionality as the full redirector but consumes less conventional memory by loading DOS LAN Services into upper memory.

Virtual Redirector: Provides the optimum memory availability since it does not use conventional memory, because it runs as a Windows virtual device driver.

Note: Even if you run the full redirector before starting Windows, the virtual redirector will load providing SYSTEM.INI has the correct statements in the [386Enh] section.

With DOS LAN Services installed on a workstation running Windows you are provided with seamless access to all of the features of DOS LAN Services from the Windows graphical user interface.

Configuration

Once you have successfully installed DOS LAN Services you may then start the requester by typing `NET START`. The following options are available, although generally do not need to be used:

Table 4. DOS LAN Services NET START Options and Initialization Process

Option	Function	Initialization Process
BASIC	Starts the basic redirector	NET.EXE executes: • NETWKSTA.EXE (within NET.EXE) • NETBEUI.EXE (within NET.EXE)
FULL	Starts the full redirector	NET.EXE executes: • REDIR.EXE (within NET.EXE) • NETBEUI.EXE (within NET.EXE)
REQUESTER	Starts the default redirector	Depends on which redirector is configured
PEER	Starts the Peer service	NET.EXE executes: • SHARE.EXE (if not already loaded) • PEER.EXE
NETBIND	Binds protocols and network card drivers	NET.EXE executes the NETBIND command
NETBEUI	Starts the NetBIOS interface	NET.EXE executes NETBEUI.EXE (within NET.EXE)
MESSENGER	Starts the Messenger service (requires the FULL redirector)	NET.EXE executes MESSENGER.EXE
NETPOPUP	Starts the Netpopup service (requires the FULL redirector and Messenger service)	NET.EXE executes NETPOPUP.EXE
/LIST	Displays a list of the requester components that have been started	Not applicable
/YES	Executes the NET START command without prompting for information or asking for confirmation of actions	Not applicable

Graphical User Interface

As previously mentioned, you may access network resources from DOS workstations by using any of the three interfaces provided by DOS LAN Services:

- DOS LAN Services graphical user interface
- Windows interface
- Command line interface (the DOS command prompt)

The graphical user interface provided with DOS LAN Services supports DBCS and mouse input. It can be used on DOS clients with or without Windows and enables you to perform the following tasks:

- Log on and log off to/from a LAN Server domain, modify logon assignments and re-establish *persistent connections*, if you have any
- Change logon password and user comment
- List users logged on to the domain
- Modify the appearance of the graphical user interface
- Share directories and printers with other users on the network
- View directory-limit information for a shared directory
- Send and receive network messages
- Define private and public applications

The DOS LAN Services graphical user interface may be run in graphics mode on any monitor/video adapter combination supporting VGA graphics or higher. The graphical user interface will gain no benefit from higher resolution graphics.

If a workstation does not support VGA, the graphical user interface may be run in text mode by specifying the /T switch after the NETGUI command.

The DOS LAN Services graphical user interface is packaged with DOS LAN Services and is presented as an installation option of DOS LAN Services. Unless otherwise specified, it is installed by default.

3.4 Windows File and Print Client (DOS LAN Services Windows Support)

When implemented on a system running DOS and Windows, DOS LAN Services enables you to access network resources through the Windows graphical user interface, as shown in Figure 74.

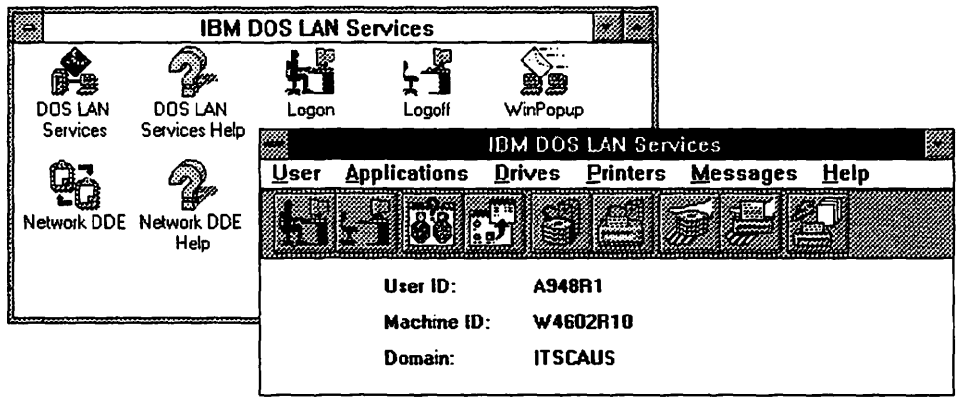


Figure 74. DOS LAN Services Windows GUI

DOS LAN Services Windows enables you to:

- Logon and logoff
- Change password
- Change user description

- View logged on users
- Modify logon assignments
- View, connect to, and disconnect from OS/2 Warp Server shared resources
- View, install and use OS/2 Warp Server shared applications
- Send and receive messages
- Manage print jobs in shared print queues
- View directory limit information for a shared directory
- Share local directories and printers

The following restrictions apply, such that you cannot:

- Define private applications
- Logon or logoff a media-less remote initial program load (RIPL) requester
- Start the virtual redirector if Windows is loaded from a network drive
- Use the BASIC redirector
- Work with Windows 32-bit file access
- Work with 32-bit NDIS VXD device drivers

Installation

When you install DOS LAN Services, as described in "Installation" on page 66, you will install Windows Support by default. If you have Windows already installed on the system then a `run = dlssetup` statement will be added to the Windows WIN.INI file which will be replaced with `run = wdls` after installation.

When you next start Windows DLSSETUP.EXE will make the following modifications to the Windows SYSTEM.INI file in the sections listed:

```
[Boot]
NETWORK.DRV=DLSNET.DRV

[Boot.Description]
NETWORK.DRV=IBM DOS LAN Services

[386Enh]
NETWORK=vnetbios.386,vnetsup.386,vredir.386
```

In addition, a DOS LAN Services program group will be created.

Notes:

1. If you install Windows on a system which already has DOS LAN Services installed you can make the above modifications by starting Windows, selecting Files from the Program Manager action bar, then select Run, and then type in C:\NET\DLSSETUP.EXE assuming that you installed DOS LAN Services with Windows Support before.
2. Even if you run the full redirector before starting Windows, the virtual redirector will load assuming SYSTEM.INI has the correct statements in the [386Enh] section.

Configuration

Following installation, DOS LAN Services may be configured via the Network program icon located in the Windows Control Panel. The DOS LAN Services Configuration window, as shown in Figure 75, enables you to modify options for logging on at startup, resource sharing, and network warnings.

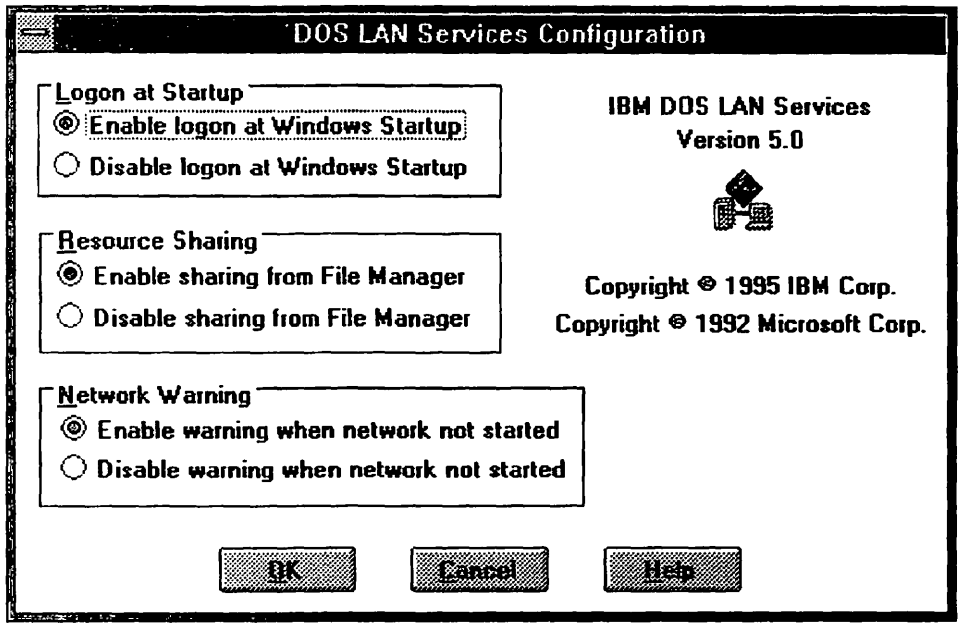


Figure 75. DOS LAN Services Windows Configuration Window

The DOS LAN Services group contains program icons to enable you to logon, logoff, start the Network DDE and Clipboard feature, and access the DOS LAN Services main window. All of the functions accessible from DOS LAN Services DOS graphical user interface are available and integrated into the Windows environment. For example, if you select the Printers pull-down menu, you are provided with direct access to the Windows Print Manager.

Customizing your DOS LAN Services Windows GUI

It is possible to customize your DOS LAN Services Windows GUI appearance and also restrict access to menu bar items by creating an optional .INI file. This is of particular use where you want to provide a standard workstation configuration tailored to enable users to perform their job whilst preventing them from modifying their logon assignments, connections, and so on.

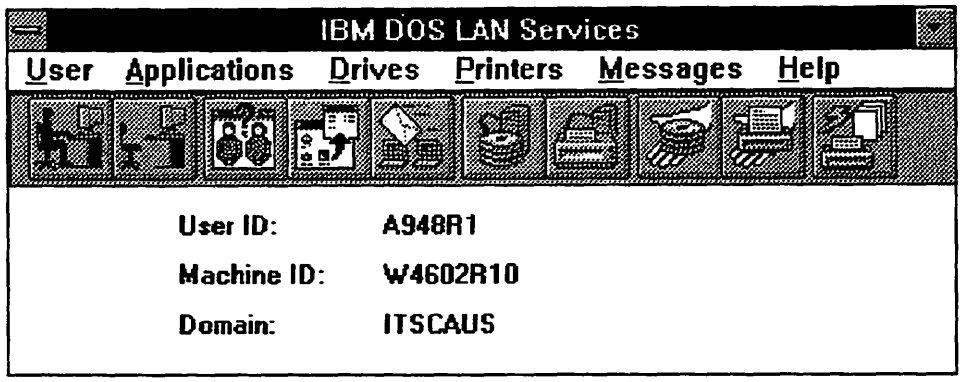


Figure 76. DOS LAN Services Windows GUI

It is also possible to hide the DOS LAN Services Windows GUI interface so that they may only logon and logoff using icons from the DOS LAN Services program group.

This has been achieved by modifying WDLS.EXE so that it automatically searches for a file called WDLS.INI in the directory where DOS LAN Services has been installed.

Note: WDLS.INI (as well as any other .INI file) can be a hidden file, enabling an administrator to reduce the possibility of a user finding the file and changing the settings.

The sample WDLS.INI in Figure 77 shows the default values.

Note: A default WDLS.INI file is *not* included with DOS LAN Services If you wish to customize your menu appearance then you need to create one. You do not need to include all default definitions just the section headings and the relevant entries that you wish to change.

```
[MenuBar]
User=1
Applications=1
Drives=1
Printers=1
Messages=1
Help=1

[MainWindow]
HideMainWindow=0
ShowNormalAtStartup=1
ShowNormalAtLogon=1
LogonAtStartup=1
Toolbar=1
```

Figure 77. Sample DOS LAN Services Customization File

Each entry in the [MenuBar] section can be used to selectively disable/enable menu bar items in the DOS LAN Services main window (provided that the service associated with the menu item is started). A value of 0 will disable the menu item (the default is to display the menu item (=1)).

If you compare the DOS LAN Services Windows GUI shown in Figure 78 on page 85 with the default GUI shown in Figure 76 you will see the results of setting the values of [MenuBar] Applications, Drives, and Printers entries and the [MainWindow] Toolbar entry to 0.

By making these modifications to the WDLS.INI file you could prevent users from modifying their logon assignments.

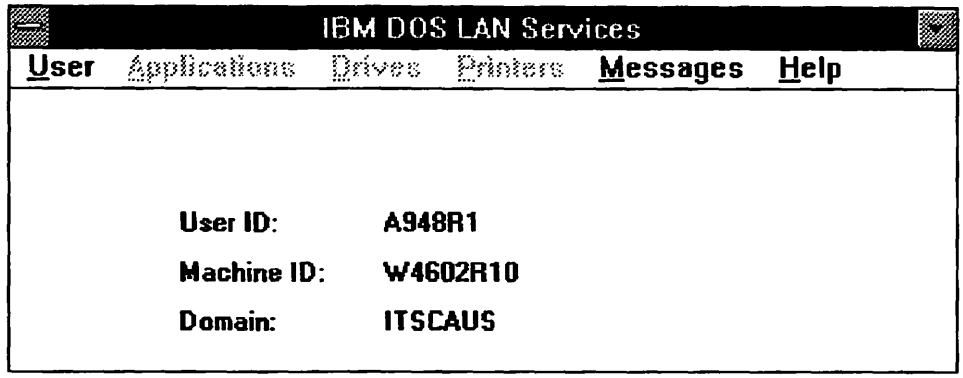


Figure 78. Customized DOS LAN Services Windows GUI

The [MainWindow] section has five entries. HideMainWindow (0=default=no) can be used to hide the DOS LAN Services main window completely. This enables you to provide only logon and logoff functions by creating program icons which call WDLS.EXE with the appropriate parameter as detailed in Table 5.

LogonAtStartup enables you to suppress the logon panel at startup if a user is not already logged on and Toolbar is used to specify whether or not a toolbar is displayed as part of the DOS LAN Services Graphical User Interface.

Table 5. DOS LAN Services WDLS.EXE Parameter Functions

Parameter	Function
0	Logon
1	Logoff
2	Start DOS LAN Services Windows Graphical User Interface
3	Manage Shared Applications
4	Change User Comment
5	Manage Drive Connections
6	Manage Printer Connections
7	Share Directories
8	Share Printers
9	Send Message

The ShowNormalAtStartup and ShowNormalAtLogon entries control how the DLS main window behaves when Windows is started and when a user logs on. The current (and default) behavior is that the DLS main window appears centered on the desktop in both situations. These entries can be set to 0 (1=default) to have the main window always minimized as an icon, until the user selects the icon, which restores the main window to the center of the desktop.

Note: If HideMainWindow is set to 1 (main window is hidden), then the ShowNormalAtStartup and ShowNormalAtLogon entries have no effect.

DOS LAN Services Windows Shared Applications

DOS LAN Services that is included with OS/2 Warp Server features enhancements to how Windows applications are accessed. Previously, RUNLSAPP.EXE, the public applications launcher for the DOS LAN Services Windows GUI, required a drive letter to be assigned to a program alias to start the Windows application.

The problem with this was that you were liable to run out of available drive letters in an environment where many shared directories and applications were being accessed.

To remove this problem, an undocumented feature of the Windows API, WinExec(), is used which accepts UNC paths for paths to programs. This enables Windows applications to be accessed in the same way as OS/2 public applications. RUNLSAPP.EXE has also been enhanced to support additional printer assignments associated with public applications.

DOS LAN Services General Hints and Tips

Attention

The additional hints and tips in this section are taken from the OS/2 Warp Server README.1ST file. Please review this file as it contains important information relating to other key OS/2 Warp Server components.

Upgrading from DOS LAN Services Version 4.0

Run TCPSTOP before installing OS/2 Warp Server client software on a workstation that already has DOS LAN Services 4.0 and IBM TCP/IP for DOS installed. If you do not stop IBM TCP/IP for DOS, a TRAP exception will occur when the INSTALL program for DOS LAN Services 5.0 starts.

Pressing Ctrl-C During NET LOGON

After running the NET LOGON command in a Windows DOS prompt, do not press Ctrl-C at the workstation password prompt. Doing so causes a general protection fault (GPF).

System Hangs Exiting Windows

If the Peer service has been started and the system hangs when you exit Windows, try increasing the size of the STACKS command in the CONFIG.SYS file.

File Copies Stop Exiting Windows

Do not exit Windows while the Peer service is running if a client is copying files from your DOS peer workstation. If you exit Windows while a copy is in progress, the copy will stop.

Memory Restrictions With Multiple LAN Transports

If you select both the NetBEUI and TCPBEUI real-mode transports when you install DOS LAN Services, you might not be able to start Windows. This is because of memory requirements below 640K. With both transports installed, Windows will not start if the Peer service is running, or if the Full redirector is running with the Messaging and Netpopup services. Windows will start if only the Full redirector and Messaging service are running.

If you install only NetBEUI or only TCPBEUI, but not both, then you can start Windows with all DOS LAN Services services running.

Extended ASCII Characters Not Supported

If you use extended ASCII characters (decimal codes 128-255) to name a network resource, users at DOS/Windows workstations might not be able to display or use that resource in DOS LAN Services in Windows or in the DOS LAN Services &guil.. This is because of the way character sets are converted for display on different workstations.

DOS LAN Services in Windows does not support extended ASCII characters (decimal codes 128-255) that do not have equivalents in the ANSI character set. This is a current restriction of Windows. Windows converts most unsupported characters to either an underscore or vertical bar. Refer to your Windows documentation for information about the ANSI character set.

On DOS LAN Services workstations that use code page 437 to display characters (primarily in the United States) the DOS LAN Services &guil. does not support the following extended ASCII codes (decimal):

155	226-229	249
157-159	231-240	251
169	242-245	252
176-224	247	254

3.5 Windows 95 Client (DOS LAN Services for Windows 95)

The DOS LAN Services for Windows 95 component allows your system running Microsoft Windows 95 to access IBM OS/2 LAN Server functions such as Aliases, Directory Limits, Shared Applications, and so on. This product is an add on to the Windows 95 Microsoft Network function. It gives you all of the LAN Server Server function, in addition to what Windows 95 provides.

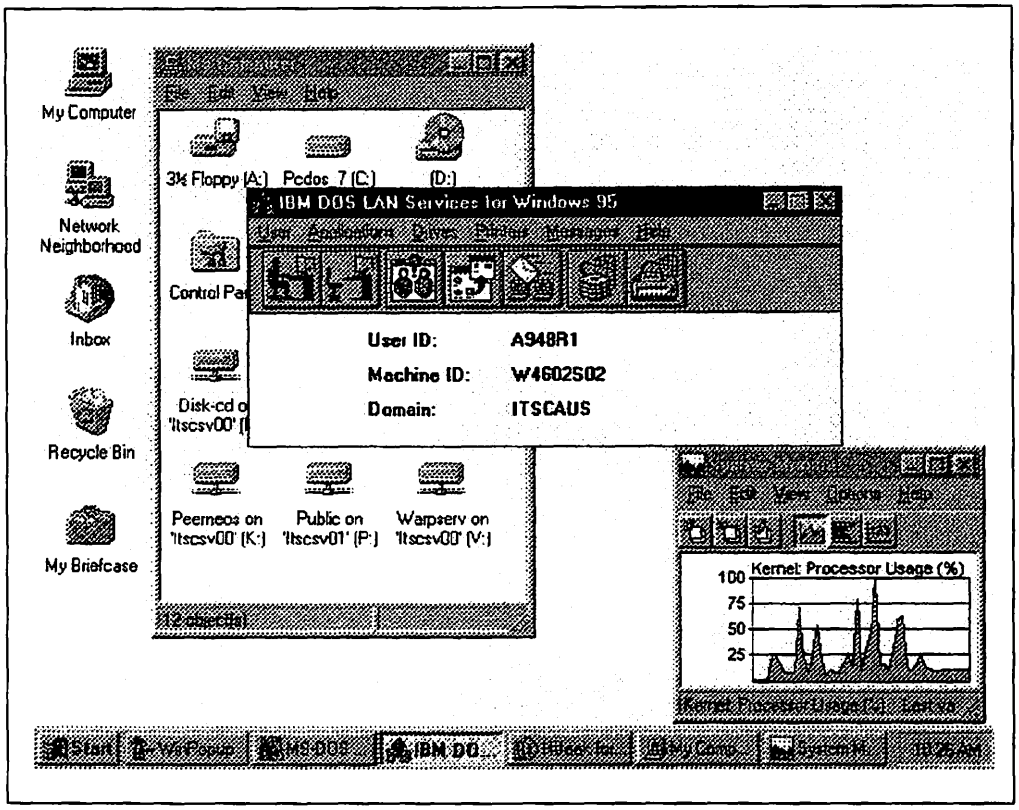


Figure 79. DOS LAN Services in a Windows 95 Environment

Installation

DOS LAN Services for Windows 95 may be installed from either a diskette created from an image on the OS/2 Warp Server CD-ROM (contents of d:\CID\CLIENT\DLS4W95) or directly from the CD-ROM.

Follow these steps to install DOS LAN Services for Windows 95 on your computer from the diskette:

1. Insert the DOS LAN Services for Windows 95 diskette into the A: drive
2. Select **Start** from the Windows 95 Task Bar
3. Select **Settings**
4. Select **Control Panel**
5. Double click on Add/Remove Programs
6. Select the tab titled Windows Setup
7. Select push button **Have Disk...**
8. Select **OK** from the Install From Disk menu
9. Check the box next to DOS LAN Services for Windows 95
10. Select push button **Install**

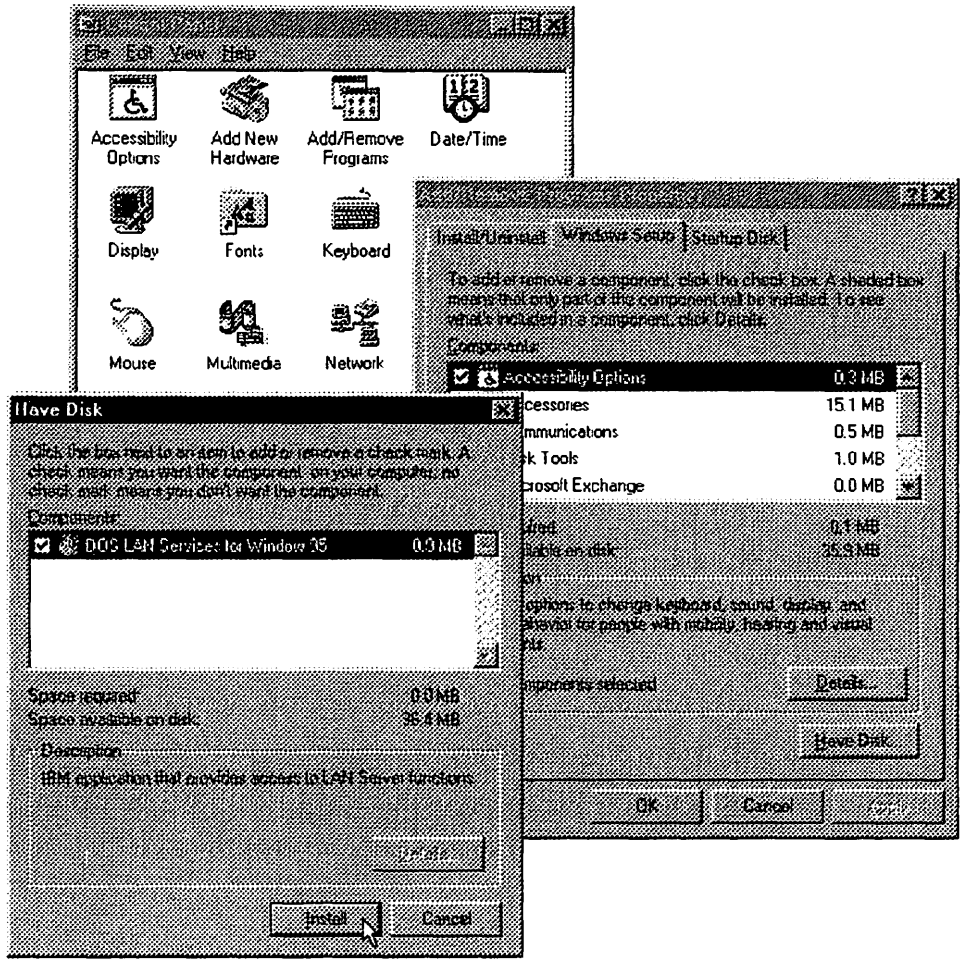


Figure 80. DOS LAN Services for Windows 95 Installation

After installation, DOS LAN Services will appear on the Task Bar in the Programs menu.

Follow these steps to install DOS LAN Services for Windows 95 on your computer from the OS/2 Warp Server CD-ROM:

1. Insert the CD ROM into your CD-ROM drive
2. Select **Start** from the Windows 95 Task Bar
3. Select **Settings**
4. Select **Control Panel**
5. Double click on **Add/Remove Programs**
6. Select the tab titled **Windows Setup**
7. Select push button **Have Disk...**
8. Type in the drive of your CD-ROM followed by the path to the DOS LAN Services for Windows 95 directory, for example:

   ```
   d:\CID\CLIENT\DLS4W95
   ```

9. Select **OK** from the Install From Disk menu
10. Check the box next to DOS LAN Services for Windows 95
11. Select push button **Install**

After installation, DOS LAN Services will appear on the Task Bar in the Programs menu.

Graphical User Interface

To start the DOS LAN Services for Windows 95 GUI select **DOS LAN Services for Windows 95** from the Program menu which you access from the Windows 95 Task Bar.

You will be presented with the DOS LAN Services for Windows 95 Graphical User Interface as shown in Figure 81.

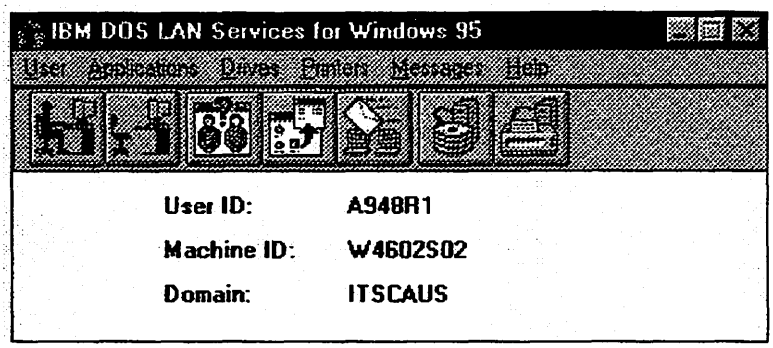

IBM DOS LAN Services for Windows 95
User Applications Drives Printers Messages Help
User ID: A948R1
Machine ID: W4602S02
Domain: ITSCAUS

Figure 81. DOS LAN Services for Windows 95 Graphical User Interface

Note: You may customize the appearance of the DOS LAN Services for Windows 95 GUI in the same way as you can for the DOS LAN Services Windows GUI as described in "Customizing your DOS LAN Services Windows GUI" on page 83.

Accessing LAN Server Functions

You access the LAN Server NET commands by using the NETLS command. This is done to supplement the Microsoft NET commands. The following commands are supported using the NETLS command from an MS-DOS command prompt:

NET ADMIN	Runs a command or starts a command processor on a server from a workstation. You must have administrative privilege at the server to use this command.
NET ALIAS	Displays a list of aliases on a specified domain or information on a specific alias.
NET DASD	Displays directory limits for the maximum usable disk space for a remote HPFS386 logical drive.
NET HELP	Provides information about commands and error messages.
NET SEND	Sends messages to other computers or users on the local area network.
NET USE	Connects to or disconnects from a shared resource or displays information about connections.
NET WHO	Lists usernames logged on in a domain or a server, and displays information about individual users.

If you would like to access all NET commands using NET.EXE you will need to run DLSNET.BAT with the parameter Y. This batch file renames the Microsoft

NET.EXE program to NET95.EXE, and NETLS.EXE to NET.EXE. The DOS LAN Services for Windows 95 NET.EXE (NETLS.EXE) will execute the commands listed in the previous section. If the command is not one of these it will send the command to the Microsoft NET95.EXE program to be processed.

The Windows 95 Network Neighborhood

For OS/2 LAN Server and OS/2 Warp Server workstations to appear in the Network Neighborhood you need to configure at least one workstation in the domain to run *File and Printer Sharing for Microsoft Networks* and act as the *Browse Master*. The workstation(s) should be modified in the following way:

1. Select **Control Panel** from the Task Bar (Start)
2. Select **Network**
3. Highlight **File and Printer Sharing for Microsoft Networks** and press the button **Properties**
4. Set the Property **Browse Master** to the Value **Enabled**
5. Set the Property **LM Announce** to the Value **Yes**
6. Select the **OK** button on the **File and Printer Sharing for Microsoft Network Properties** panel
7. Select the **OK** button on the **Network** panel

Once you have completed these steps you need to restart the system to activate the changes.

Sharing Restrictions in non-NT Domains

If you log on to a non-NT domain or workgroup from a Windows 95 peer workstation, you can use only share-level access control for shared files and printers. If you attempt to set user-level access, the list of users cannot be displayed.

3.6 Installing and Running DOS LAN Services on OS/2

Previously it has not been possible to use the DOS LAN Services Windows network driver (DLSNET.DRV) with WIN-OS/2 and VNETAPI.OS2 and you have had to resort to the Microsoft LAN Manager 2.x Windows network driver (LANMAN.DRV) in order to communicate with LAN Server. However, LANMAN.DRV does not have support for browsing and connecting to aliases, running public applications, and so on. If you wanted to connect to an alias for you to use in a WIN-OS/2 session, you had to switch to OS/2, make the connection, then switch back to the WIN-OS/2 session. Also you could not run a public application from within a WIN-OS/2 session.

Incompatibilities between DLSNET.DRV and VNETAPI.OS2 have been resolved and design changes to the Windows GUI have made it compatible with VNETAPI.OS2. This now provides users of OS/2 LAN Requesters the ability to connect to LAN Server resources from each WIN-OS/2 session without having DOS LAN Services installed and enables them to run DOS and Windows public applications from each WIN-OS/2 session. A full installation of DOS LAN Services is not required, only the DOS LAN Services Windows program files and drivers are required.

Note: This implementation removes the requirement for DOS LAN Services to run in each WIN-OS/2 session, since VNETAPI.OS2 *virtualizes* the LAN Server APIs called by DLSNET.DRV, thereby conserving system memory and adapter resources.

Installing DOS LAN Services on OS/2

The following procedure describes how to set up your system to access network resources (aliases or netnames), and network applications from a WIN-OS/2 session. This procedure installs the drivers and code needed to support the DOS LAN Services Windows interface. By using the DOS LAN Services Windows drivers and Windows GUI, you will have access to many functions usually available only when the full DOS LAN Services product is installed. Network functions within the WIN-OS/2 File Manager and Print Manager are also enabled within each DOS session, including the ability to browse network resources, and manage print jobs on remote queues.

Before beginning this procedure, check to see that you have the following prerequisite software installed:

- WIN-OS/2 (provided with OS/2)
- OS/2 LAN Requester
- Virtual DOS LAN API Support (VNETAPI.OS2, by default, is installed with OS/2 LAN Requester).

If you need to install OS/2 LAN Requester or the Virtual DOS LAN API Support option, use the Advanced LAN Services Installation/Configuration path to do so before continuing with this procedure (see Figure 5 on page 12).

The following steps explain how to complete your setup by installing the DOS LAN Services Windows drivers and Windows GUI code needed for your WIN-OS/2 session:

- To install the DOS LAN Services Windows drivers and Windows GUI code to run with Virtual DOS LAN API Support:

  1. From an OS/2 command prompt type:

     ```
     VNETDLS
     ```

     Note: Type `VNETDLS /?` or `VNETDLS HELP` to see the valid parameters and syntax for this command.

  2. Follow the instructions displayed on the panels; you will be prompted to provide configuration information.

     The program installs the required DOS LAN Services Windows files from either diskette or CD-ROM to your hard-disk.

Notes:

1. DLSSETUP.EXE builds the DOS LAN Services program group in WIN-OS/2 and creates the program icons for DOS LAN Services and DOS LAN Services Help.
2. If you install the DOS LAN Services Windows drivers and Windows GUI in a specific DOS session, you must also load VNETAPI.SYS. This differs from systems running native DOS LAN Services on OS/2 LAN Requester, where VNETAPI.SYS should not be loaded in the same session.
3. If you have DOS or Windows applications that require NetBIOS or 802.2, install the appropriate virtual device driver, using LAPS. For more

information, refer to the *MPTS-Configuration Guide* which is available online and resides in the LAN Services File and Print folder within the Information folder.

The Windows interface provided with the DOS LAN Services Windows drivers does not offer all the functions of native DOS LAN Services. The following functions are not available from the Windows interface running with VNETAPI.OS2. These functions are only available if you have installed DOS LAN Services in a specific DOS session (on OS/2) or on a DOS workstation:

- Logon or Logoff
- Share directories and printers
- Change workstation password
- View message log
- Change log file or device
- Enable and disable message logging
- WinPopup
- Network DDE

Refer to *DOS LAN Services and Windows User's Guide*, available online, for information about these other functions provided with DOS LAN Services.

Connections made or deleted using the Windows interface running with VNETAPI.OS2 are displayed as network connections in both OS/2 and WIN-OS/2 sessions. For example, if you make a connection to an alias from a WIN-OS/2 session, then switch to the OS/2 command prompt and type NET USE, the new connection to the alias will be listed. Similarly, any connections made using the OS/2 LAN Requester will be reflected in your WIN-OS/2 session. This behavior differs from systems running native DOS LAN Services under OS/2, in which the connections (or disconnections) are not reflected in other OS/2 and WIN-OS/2 sessions.

Attention

The DOS LAN Services Windows interface can also be used with Virtual DOS LAN API Support on OS/2 LAN Servers, except LAN servers configured as Domain Controllers.

3.7 Connecting to Network Resources from DOS LAN Services

DOS LAN Services enables you to use directories across the network. These directories, called shared directories, are used the same way that disk drives and directories are used on your workstation. You can use files and application programs on the shared directory at your workstation as though they were stored on your hard disk. When you use a shared directory, you establish a session, or connection to, that directory. You can establish connections that start automatically each time you log on to the network. These automatic connections are known as persistent connections and logon assignments.

Persistent connections are stored locally on the workstation and can be different for each workstation. Each user logging on to the same workstation has the same connections even though their user IDs are different. Connections occur regardless of the type of logon, for example, local and domain. At logon, you are only connected to the persistent resources to which you were connected the

last time you were logged on. For example, if you disconnect from a drive resource, you are not automatically reconnected the next time you log on.

Logon assignments are based on user IDs. They are stored on the LAN Server domain controller as part of the domain controller database (DCDB). They can be different for each user, and a user logging on to different workstations has the same connections. Connections occur only with a domain logon.

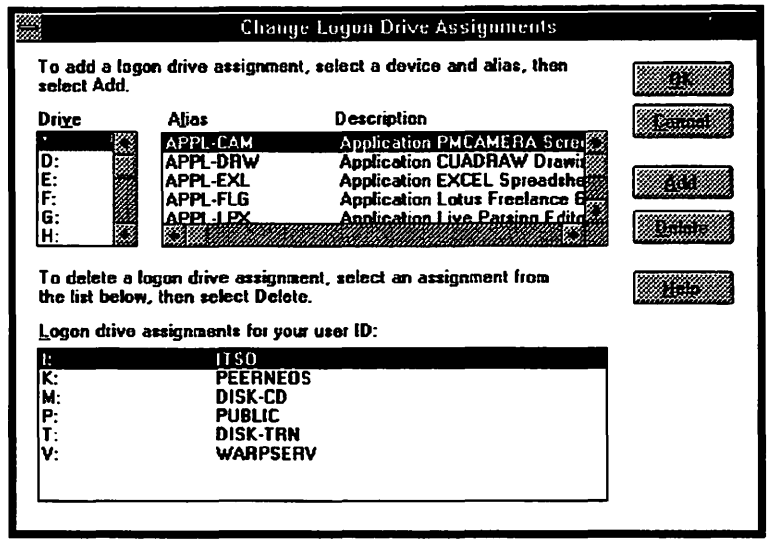


Figure 82. Changing Logon Drive Assignments

Persistent connections and logon assignments are not mutually exclusive. You can have both; however, persistent connections are done first, and you may run into conflicts with drive and printer assignments.

An alias is a nickname for a resource. For example, an alias of APPS can be created to refer to a directory on SERVER1 named C:\NETWORK\APPS. After an alias is assigned by a network administrator, you can refer to the directory simply as APPS. After an alias is assigned to a resource, you do not need to specify the server where the resource is located or the path to the resource. An alias remains defined after the domain controller is stopped and restarted.

As an alternative, a resource can be temporarily defined by a netname. When combined with the name of the server on which the resource is located, the netname identifies a shared resource on the server. For example, a directory with a netname of TRANSFER on SERVER1 is referred to as:

```
\\SERVER1\TRANSFER
```

The combination of a server name and a netname is called a network path. Unlike an alias, a netname does not remain defined if the server is stopped. When you connect to a resource using a netname, you must specify the server name.

3.8 DOS LAN Services Logon Process

In this section we will look in detail at the sequence of events that follow the execution of a logon request from a DOS client running DOS LAN Services.

When DOS LAN Services receives a logon request the following process is invoked:

1. If the user is not allowed to logon to multiple requesters with the same user ID (`multilogon=no` is specified in NETWORK.INI) and their ID and the domain name are both less than or equal to eight characters in length then the user ID/domain NetBIOS name is added to the network adapter to ensure that the user is not logged on elsewhere.

   Note: The format of the NetBIOS name is a eight character long user ID padded with blanks followed by an eight character domain name padded with blanks.

2. If `lslogon=yes` is specified in NETWORK.INI and either the Full or Virtual redirector are loaded NETWKSTASETUID2 is called to logon the user and validate the user ID and password.

3. The NETUSERGETINFO API is then called to determine if the user has a home directory:

   - If the user has a home directory, a connection is made to it and it is assigned as the current drive.
   - The NETUSERGETLOGONASN API is called to get the user's logon assignments.
   - If an error is received that indicates that the domain control database (DCDB) has not been initialized:

     NETUSERDCDBINIT is called to initialize the DCDB

     NETUSERGETLOGONASN is called again

     User's logon assignments are being retrieved

   - If an error is received that indicates a downlevel server:

     A check is made to determine whether an \IBMLAN\DCDB\USERS*userid* directory exists. If not a logical server call is made to create it.

   - Redirected I/O is then used to obtain the user's logon assignments (the NETSHAREGETINFO API is issued to get the server and network name of the alias, then an INT21H call redirects the device, filesets first, then printers)
   - The user logon script (PROFILE.BAT) is then executed if one exists
   - If `timesync=yes` is specified in NETWORK.INI the NETREMOTETOD API is called to get the time from the domain controller and set it locally on the workstation

4. If `lslogon=no` is specified in NETWORK.INI or the Basic redirector is loaded NETWKSTASETUIDQUICKLY is called to register the user ID and password without validating at the server

5. Persistent connections are connected to

6. If the Messenger service is started then a listen NetBIOS command is issued

7. If the current drive is redirected then it is changed to the drive where DOS LAN Services is installed

As is to be expected, the logoff process is less involved. When you log off the following occurs:

1. The NETWKSTASETUID2 API is called to log the user off the domain. This API is also responsible for cancelling all disk and print redirection
2. The user ID/domain NetBIOS name is then deleted

Local Logon

You can perform both a local logon and a domain logon. To access peer resources, only a local logon is necessary. If your user ID and password are the same both locally and on the domain, then a local logon also allows you access to domain resources; however, you must provide the netname (\\server\sharename) when making the server connection, because aliases are not interpreted with a local logon. In order to use aliases, you must be logged on to the domain.

With only a local logon and no domain logon, you do not receive your domain logon assignments. However, DOS LAN Services will attempt to reconnect any persistent connections for that workstation. If your user ID has permission to use these reconnected resources, then you will be granted access. If you do not have permission, then the connection may be made (for example, drive LPT1 may connect to IBM4039), but you could then not actually use the resource.

For each user that logs on at a workstation, DOS LAN Services maintains an unreadable password file with the extension PWL. This file contains a local password, domain password (if the user has logged on to a domain), and peer service password (if the user has used peer resources requiring passwords).

3.9 Sharing Requester Resources with the Peer Service

OS/2 LAN Requester has been available with peer capabilities since OS/2 LAN Server Version 3.0 and has been well documented. DOS LAN Services, initially introduced in OS/2 LAN Server 4.0, includes a peer service which has been further enhanced in OS/2 Warp Server.

The DOS LAN Services Peer service allows you to share the resources of your DOS workstation with other OS/2 Warp Server clients and other Server Message Block (SMB) based network products.

As a server, a DOS LAN Services peer workstation with user level security has the following features:

- A DOS LAN Services peer workstation can share local disks, directories and printer queues.
- A DOS LAN Services peer workstation maintains it's own user account database and access control lists (see "User Level Security" on page 98). It controls access to it's local resources based on this user account database and access control lists. Unlike LAN Server, the peer workstation's user account database is not synchronized with any other user accounts database.

The user security function of DOS LAN Services provides additional NET commands and APIs, to administer user accounts and access control lists, for local and remote administration respectively.

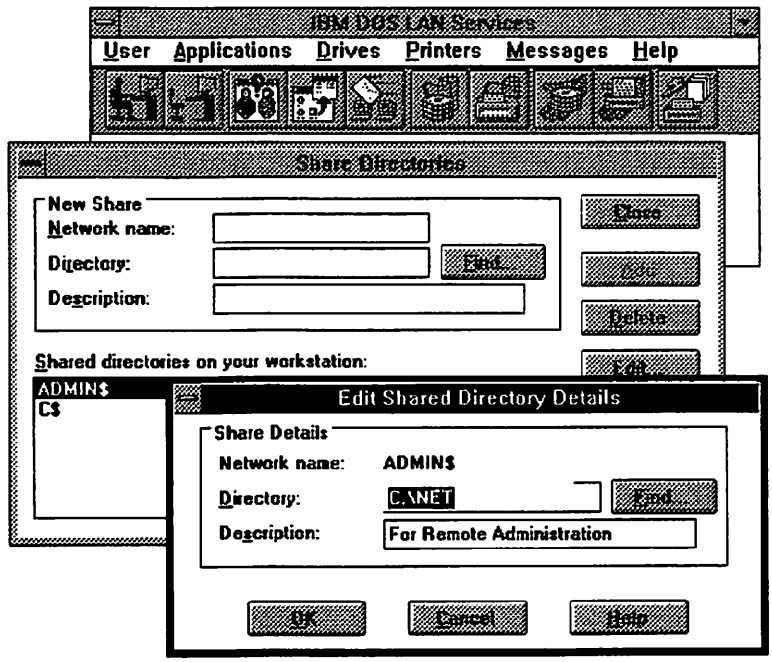


Figure 83. Sharing a Directory with DOS LAN Services Peer Services

The following restrictions apply to the DOS LAN Services Peer service:

- The following resources may *not* be shared by a DOS LAN Services peer workstation:
  - Serial devices
  - Named pipes
  - Mailslots (class 1)
  - CD-ROM drives
- The DOS LAN Services peer workstation will only support a single connection at any one time. This is the single session restriction that also applies to the OS/2 LAN Requester Peer service.

  Full unrestricted peer capability is provided by the OS/2 Peer component of the OS/2 Warp Connect product.
- The DOS LAN Services peer workstation does *not* support auditing or error logging
- A DOS LAN Services peer workstation cannot handle logon requests
- The following functions related to the logon process are *not* available at the DOS LAN Services peer workstation:
  - Establishment of logon assignments
  - Execution of a logon profile
  - Execution of a logon script
  - Establishment of home directory assignment

- The following LAN Server domain related functions are *not* available at a DOS LAN Services peer workstation:
  - Aliases for shared resources
  - Public applications
  - Remote IPL workstation support
- A DOS LAN Services peer workstation operates as a *hidden server*, such that it does not appear visible to the `NET VIEW` command nor the NetServerEnum2 API.
- A DOS LAN Services peer workstation may not be remotely administered using the `NET ADMIN` command (you will receive a SYS0050 error and be informed that the network request is not valid).

  The only way to remotely administer a DOS LAN Services peer workstation is by issuing remote API calls (see "Peer User Level Security APIs" on page 101).
- The DOS LAN Services Peer service does *not* support opportunistic locking

Additional restrictions are detailed in "Peer Administration Considerations" on page 100.

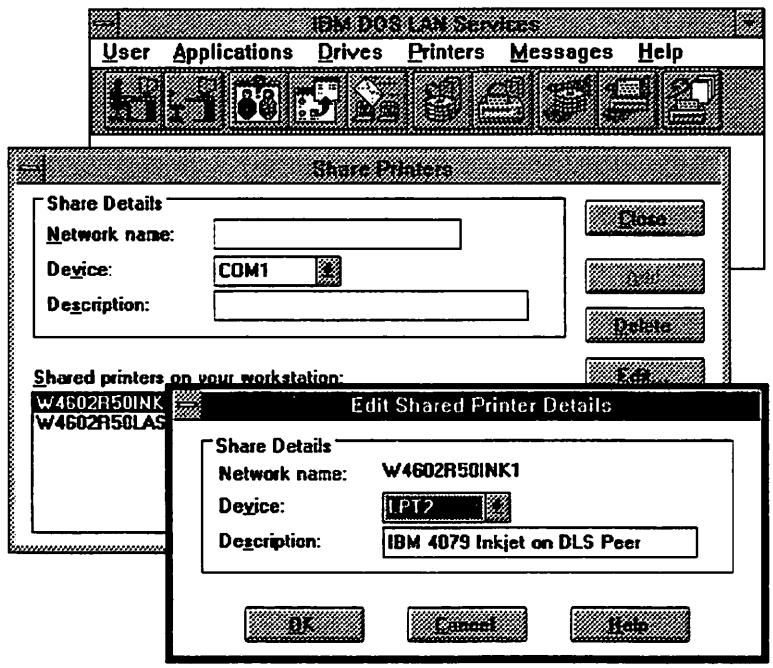


Figure 84. Sharing a Printer with DOS LAN Services Peer Services

User Level Security

DOS LAN Services, as included with OS/2 Warp Server, provides you with the ability to define access control profiles for shared resources located on the local workstation. Previously, the only method of defining access to shared DOS and Windows workstation resources was via *share level security*. Share level security allows you to specify both the password and permissions associated with a shared resource *not* the user.

Now *user level security* allows you to define access to shared resources located on DOS and Windows workstations at a user and group level. OS/2 Warp Server File and Print Sharing Services uses this form of security, which is also the default security mode for OS/2 peer services.

User level security is implemented in DOS LAN Services by providing access to the following NET commands:

- NET ACCESS

  Lists, adds, changes, deletes, and applies access control profiles, and also revokes specific permissions in access control profiles. An administrator can perform all actions, and a user with P permission can perform all actions for access control profiles except for the ADD and APPLY actions.

  Note: Access control profiles created by NET ACCESS are stored in the \NET\ACL.ACC file.

- NET GROUP

  Displays the names of groups and their members, updates the group list, and adds and deletes groups (for administrators and users with accounts operator privilege).

  Note: The list of groups and their members is stored in the \NET\NET.ACC file.

- NET USER

  Lists, adds, removes, and modifies user accounts in the peer workstation user account database.

  Notes:

  1. To make changes to the user accounts, this command must be run from a peer workstation.
  2. Only an administrator or user with accounts operator privilege (as defined in the local accounts database) can use this command. Users with accounts operator privilege cannot add and manage administrators or other users with accounts operator privilege.
  3. Peer workstations maintain a separate user accounts database locally that is different from the domain's user accounts database.
  4. Be careful when setting EXPIRES to a specific date. DOS LAN Services Peer service users cannot reset passwords once they have expired. The peer workstation administrator must reset the password and expiration date for the user. For the same reason setting PASSWORDEXP to YES is not recommended.
  5. The list of users is stored in the \NET\NET.ACC file.
  6. When a user is added to the peer workstation user accounts database, the user is automatically added to a group (USERS, ADMINS, or GUESTS, depending on the privilege level assigned), but if the user name has an associated password, that password is required for logon. Setting /PASSWORDREQ to NO also means that other password restrictions, including PASSWORDCHG, are not applied.
  7. Users with accounts operator privilege cannot create or modify administrator or other operator accounts.

8. Passwords are checked for restrictions only when they are changed or added. Therefore, when you change a password from being not required (PASSWORDREQ:N) to required (PASSWORDREQ:Y), the password is not checked against the minimum password limitation of four characters.

For the complete syntax of the above commands, and some examples of their use, please refer to the *DOS LAN Services and Windows User's Guide* included with the OS/2 Warp Server package.

Peer Administration Considerations

You can administer the DOS LAN Services Peer service though a command line interface. A graphical user interface is *not* provided to administer a peer workstation. To administer a peer workstation, you must be defined as an administrator in the peer workstation local user accounts database (see "User Level Security" on page 98).

It is common for the owner of a peer workstation to be defined as an administrator on the peer workstation but defined as a user on the domain. The peer administrator can manage resources for only the peer workstation, but not the rest of the domain.

Centrally Administering Peer Workstations

Since the peer workstation is not part of an OS/2 Warp Server domain, it cannot be administered through the OS/2 Warp Server Administration Graphical User Interface. This makes it relatively difficult to administer centrally.

This clearly illustrates the advantages of a server-based solution, provided with OS/2 Warp Server, over peer-to-peer networking functions provided with a product such as Microsoft Windows for Workgroups.

If you decide to set up and centrally administer the peer workstations in the network, support will be necessary for the following responsibilities:

- Installation of peer workstations
- Set up of the peer workstations with printer and file sharing
- Set up and maintenance of user accounts and group accounts for user-level security

The following are other considerations you should keep in mind before setting up or using the DOS LAN Services Peer service:

- You cannot remotely administer the DOS LAN Services Peer service by using the `NET ADMIN` command. You must use remote API calls to remotely administer the service from other workstations on the network (see "Peer User Level Security APIs" on page 101).
- Aliases, applications, serial devices, mailslots and named pipes are *not* supported and cannot be shared from peer workstations.
- The peer workstation maintains its own user account database and access control lists in order to control access to its resources (see "User Level Security" on page 98). The peer workstation's user account database and access control lists are not synchronized with the server domain's lists.

- Users and groups on the following types of requesters can access resources on a peer workstation if they are defined and have been granted access permissions:
  - DOS LAN Services
  - OS/2 LAN Requester
  - DOS LAN Requester (from LAN Server 3.0 and prior)
  - IBM PC LAN Program (PCLP) Basic
  - Microsoft LAN Manager (OS/2 and DOS)
  - Microsoft Windows for Workgroups
  - Microsoft NT
  - Microsoft Windows 95
- A peer workstation cannot act as a logon server, since it cannot handle logon requests.
- When you install the DOS LAN Services requester, the Peer service is automatically installed on the workstation, but is not automatically started. You must use the `NET START PEER` command, or add PEER to the *autostart* parameter in NETWORK.INI, to start the DOS LAN Services Peer service.
- Peer workstations are hidden servers and not viewable through the `NET VIEW` command or the NetServerEnum2 API.

Default Peer Administration User ID and Password

The user ID and password that you specify when you install DOS LAN Services is not granted administrator privileges.

To administer your peer workstation you must first logon using a default user ID (USERID) and password (PASSWORD). To avoid any security exposure it is recommended that you then create a a new administrator user ID (or define the user ID that you specified at installation as an administrator) and delete the default.

If you ever forget your administration user password you will have to reinstall DOS LAN Services.

Peer User Level Security APIs

The user level security feature of the DOS LAN Services Peer service provides the following categories of application programming interfaces (APIs) to allow a user with appropriate privileges to administer resources on the peer workstation, user accounts database and access control lists:

- Peer workstation administration APIs, notably:
  - Share APIs
  - Session APIs
- Protection APIs
  - Access APIs
  - User APIs
  - Group APIs

Differences between DOS LAN Services and OS/2 LAN Server's Corresponding APIs

This section will look at the differences between the two sets of APIs and discuss the exceptions.

Note: If an API category is ommitted in this section it is because the API functions and calling conventions are the same regardless of whether you are writing DOS LAN Services or OS/2 LAN Server code.

- **Access APIs**
  - NetAccessEnum

    When level 1 is selected, the auditing bits (USHORT acc1_attr) does not have any meaning because the DOS LAN Services peer workstation does not support the auditing function.
- **User APIs**
  - Data Structure

    Some fields of data structures are *not* supported by the user level security function of DOS LAN Services which *are* supported by OS/2 LAN Server. They are as follows:

    Structure user_info_1:

Table 6. Differences between the DOS LAN Services and OS/2 LAN Server APIs (Structure user_info_1)

Member Name	Difference in Comparison to OS/2 LAN Server's Definition
char far*usri1_homedir	The value must be *NULL*. The DOS LAN Services peer does not support home directories.
USHORT usri1_flags	The bit of UF_SCRIPT(0x01, logon script bit) and UF_HOMEDIR_REQUIRED(0x08) must be zero.
char far*usri1_script_path	Must be *NULL*.

Structure user_info_2:

Table 7. Differences between the DOS LAN Services and OS/2 LAN Server APIs (Structure user_info_2)

Member Name	Difference in Comparison to OS/2 LAN Server's Definition
char far*usri2_parms	Must be zero.
long usri2_last_logon	A value 0 is always set.
long usri2_last_logoff	A value 0 is always set.
ULONG usri2_max_storage	DOS LAN Services ignores this field. A value of -1 is returned.
USHORT usri2_units_per_week	DOS LAN Services ignores this field.
UCHAR far*usri2_logon_hours	Must be *NULL*.
USHORT usri2_bad_pw_count	The value 0xffff is always returned
USHORT usri2_num_logons	The value 0xffff is always returned
char far*usri2_logon_server	Must be *NULL*.

  - NetUserSetInfo

The valid parmnum values are:

Table 8. Differences between the DOS LAN Services and OS/2 LAN Server APIs (PARMNUM)	
parmnum **Symbol**	**Corresponding Field Name**
PARMNUM_PASSWD	usri2_passwd
PARMNUM_PRIV	usri2_priv
PARMNUM_COMMENT	usri2_comment
PARMNUM_USER_FLAGS	usri2_flags
PARMNUM_AUTH_FLAGS	usri2_auth_flags
PARMNUM_FULL_NAME	usri2_full_name
PARMNUM_USR_COMMENT	usri2_usr_comment
PARMNUM_ACCT_EXPIRES	usri2_acct_expires
PARMNUM_COUNTRY_CODE	usri2_country_code
PARMNUM_CODE_PAGE	usri2_code_page
0	all user_info_2 structure

- Group APIs

  The user level security function of DOS LAN Services has the following three built in groups which may *not* be edited by APIs.

Table 9. DOS LAN Services Built In Groups	
Group Name	**Member**
admin	All accounts with USER_PRIV_ADMIN
user	All accounts with USER_PRIV_USER
guest	All accounts with USER_PRIV_GUEST

3.10 Performance Tuning

The default installation parameter values have been selected to provide the optimum performance/memory utilization ratio. The DOS LAN Services autocache parameter, when set to yes automatically allocates the values of numbigbuf, sizbigbuf and extraheap based on the amount of XMS memory available. However, if a performance problem is identified then you may set autocache to no and manually adjust the values of the following parameters:

Work Buffers are used to construct SMBs prior to their delivery to the server. The sizworkbuf parameter specifies the size of work buffers; however, this value rarely needs to be changed because small data read requests are processed via the cache provided with big buffers.

Big Buffers are used, as with previous versions of requesters, to process large file transfers. However, with DOS LAN Services, they are now also used for file caching which provides an obvious performance advantage.

Notes:

1. Setting autocache to yes consumes 10KB of conventional memory.
2. The autocache parameter is not applicable if you are using the virtual redirector. The virtual redirector uses 1/8 of free XMS memory for buffer allocation.

3.11 DOS LAN Services Module Descriptions

The following table outlines the function of each individual DOS LAN Services module.

Table 10 (Page 1 of 2). DOS LAN Services Module Descriptions

Module	Function
DOSNET.LIB	LAN Server APIs for DOS Applications
INSTALL.BAT	Installation batch file
INSTAL16.EXE	Protected mode installation program
INSTALR.EXE	Real mode installation program
INSTALL.MSG	Installation error/warning messages
NETWORK.INF	Used by installation program to configure network adapters
NETWORK.INI	Contains the default parameters used by NET START and other services
NET.EXE	Contains the following services: • Start code, for example NET START *service name* • Redirector • NetBEUI • Loader • Spawns CMDS.EXE (command line interface (CLI)) • Spawns CMDS16.EXE (protect mode CLI)
NET.MSG	Contains error/warning messages used by all interfaces, all numbers up to three digits are prefixed with 'Error', such as 'Error 123', and all four digit numbers are prefixed with 'NET', such as 'NET1234'
NETH.MSG	Cause/action descriptions for error/warning messages in NET.MSG; message numbers between 'NET1' and 'NET7450'
CMDS.EXE	Command line interface; spawned by NET.EXE
CMDS16.EXE	Protect mode command line interface; spawned by NET.EXE
DLSHELP.SYS	Redirector helper module. Hooks interrupts and passes requests on to the redirector
PEER.EXE	Peer service module; provides local file and print sharing capabilities
PQ.SPL	Print queue management file used by Peer service
PQ.SEP	Separator page used by Peer service for shared printers
NETGUI.BAT	Starts the DOS graphical user interface and reloads it after running an application
DZG4.EXE	Actual DOS graphical user interface executable
SUPPORT.DAT	Contains all DOS graphical user interface panels for both graphics and text modes

Table 10 (Page 2 of 2). DOS LAN Services Module Descriptions	
Module	**Function**
GUI.MSG	Error/warning messages used by DOS graphical user interface and WDLS.EXE (Windows GUI); message numbers between NET7450 and NET7600
GUIH.MSG	Cause/action text for error messages in GUI.MSG
MOUSE.DLL	DLL used by DOS graphical user interface for protected mode mouse support
CONNECT.DAT	Stores persistent connection information (see 3.7, "Connecting to Network Resources from DOS LAN Services" on page 93)
userid.PWL	Password list file for a particular user ID; stores passwords for connections and logon
NETPOPUP.EXE	Provides message popup
MESSENGR.EXE	Receives messages and either logs them or passes them on to NETPOPUP.EXE
MESSAGES.LOG	Default message log file
CONNECT.TXT	DOS LAN Services troubleshooting document
WDLS.EXE	DOS LAN Services Windows interface
DLSNET.DRV	DLL used by WDLS.EXE (do not be confused by the extension)
DLSNET.HLP	DOS LAN Services Windows help file
NETAPI.DLL	LAN Server APIs for Windows applications
PMSPL.DLL	LAN Server print APIs for Windows applications
RUNLSAPP.EXE	Invokes WinExec() function to run applications
WINDLS.DLL	DLL used by WDLS.EXE, DLSNET.DRV and RUNLSAPP.EXE
WINPOPUP.EXE	Interacts with NETPOPUP.EXE to display messages in a Windows environment
DLSSETUP.EXE	Modifies WIN.INI and SYSTEM.INI files to provide Windows support by pointing to DLSNET.DRV (see "Installation" on page 82)
FMSHARE.DLL	Hooks into Windows File Manager for directory sharing when the DOS LAN Services Peer service is active
VNETBIOS.386	Real mode to protect mode NetBIOS layer used by the virtual redirector (VREDIR.386)
VNETSUP.386	Virtual redirector support module used for reading .INI information and initialization of the redirector
VREDIR.386	Virtual redirector used in Windows enhanced mode

3.12 DOS LAN Services Common Configuration Scenarios

In the previous sections we have discussed DOS LAN Services in an IBM NetBEUI environment. This is the default protocol driver automatically set by the installation program. This protocol is faster than 802.2 but uses more memory. All redirectors can be used with this option.

In this section we will look at some of the various scenarios covering the wide range of connectivity options provided with DOS LAN Services.

As shipped with OS/2 LAN Server 4.0, DOS LAN Services TCP/IP support was provided by packaging a TCP/IP 2.1.1 for DOS Stack Kit with the product. You

needed to install DOS LAN Services and *then* install the TCP/IP Stack Kit. DOS LAN Services provided with OS/2 Warp Server now includes an integrated TCP/IP stack which is selectable when you install DOS LAN Services and choose to change the default protocol driver from the default IBM NetBEUI. When you do this you are presented with the following options:

- Other Protocol
- 802.2 Support
- TCPBEUI (Real-Mode)
- TCPBEUI (Real-Mode) and IBM NetBEUI
- TCPBEUI (Windows Protect-Mode)
- TCPBEUI (Windows Protect-Mode) and IBM NetBEUI
- IBM NetBEUI

In the following sections we will discuss the reasons for selecting each of the different protocols.

Other Protocol

If you have diskettes from another source (such as the manufacturer of the adapter) you would select this option if you have an OEM protocol driver.

802.2 LAN Transport

Loads the LAN Support Program drivers for 802.2. This protocol uses less memory, but runs slower than NetBEUI. 802.2 support must be installed on DOS workstations using remote IPL. This protocol contains LAN Support Program code, which makes it possible to install the LAN Support Program separately. All redirectors can be used with this option.

TCPBEUI (Real-Mode) LAN Transport

Provides NetBIOS over TCP/IP (see 6.2, "NetBIOS over TCP/IP on OS/2 Warp Server" on page 260 for a definition). The real-mode drivers reside under the real memory (first 640K). You require File and Print Sharing Services with TCPBEUI on the server. This protocol can be used for environments that require TCP/IP only. All redirectors can be used with this option.

TCPBEUI (Real-Mode) and IBM NetBEUI

This option provides two protocols. It provides TCP/IP and Networking capabilities. Depending on your constraints, you might not be able to run netpopup or peer servers, and then start Windows. If you have Windows for Workgroups installed, use TCPBEUI (Windows Protect-mode) and IBM NetBEUI. All redirectors can be used with this option.

By default, this option assigns NetBEUI to LAN adapter 0. The messenger, netpopup, and peer servers can only use adapter 0, therefore, they will only be able to communicate with the other workstations running NetBEUI. To enable these servers to talk to workstations running TCPBEUI, you must configure TCPBEUI for adapter 0.

TCPBEUI (Windows Protect-Mode) LAN Transport

This option can only be used with Windows for Workgroups. It provides TCP/IP over NetBIOS without using real memory (first 640K). To use messaging, netpopup (or Winpopup), and peer services (these services are started using the command line interface), use TCPBEUI (Windows Protect-mode) and IBM NetBEUI. You need to use virtual redirector with this option.

TCPBEUI (Windows Protect-Mode) and IBM NetBEUI

This option requires Windows for Workgroups and provides two protocols. All redirectors can be used with this option.

By default, this option assigns NetBEUI to LAN adapter 0. The messenger, netpopup, and peer servers can only use adapter 0, therefore, they can only communicate with other workstations running NetBEUI. To enable these servers to talk to workstations running TCPBEUI, you must configure TCPBEUI for adapter 0.

TCPBEUI Configuration

If you selected a TCPBEUI protocol driver, you will be prompted for the following TCP/IP configuration information:

- IP Address
- Net subnet mask
- Gateway address
- Domain Name server address

If you choose TCPBEUI support, IP address and Net subnet mask address are needed to start DOS LAN Services after installation. For a definition of the above parameters you should refer to 5.2, "Installing TCP/IP Services" on page 171.

DOS LAN Services TCPBEUI Utilities

If you have chosen TCPBEUI support the following tools are provided to assist you in determining the source of communication problems and creating a local name cache.

Using the Ping Program

If you are going to send a file to another host, you can ping a host to see if it is connected to the network. In another case, if you try to connect to a gopher server and you get no response, try to ping the gopher server. The Ping program can be used to test your connections throughout the network if you are having trouble communicating with another host. A host might not respond to a ping, however, for the following reasons:

- A host might be inoperative.
- A gateway between you and the host might be inoperative.
- The host might be slow to respond.
- The data length might be too large for the host to receive.
- You are using a TCP/IP protocol stack not provided with this product.

Try using additional pings to communicate with other hosts in the network. To determine the location of the failure, you need to know the topology of the network.

You should issue pings in the following order, until the failure is located:

1. Send a ping to your local host.
2. Send a ping to a host on your local network.
3. Send a ping to each intermediate node that leads from your local host to the remote host, starting with the node closest to your local host.

The ping program might not run correctly if you are using a TCP/IP protocol stack provided by another vendor. The ping program uses raw socket calls and therefore is tied to the stacks provided by IBM.

The format of the PING command is:

```
ping [-l datalen] [-n count] hostname
ping hostname [-l datalen] [-n count]
```

where:

`-l datalen` Is the size of the ICMP data to send

`-n count` Is the number of the ICMP requests to send

`hostname` Is the remote name or dotted decimal IP address

You may also use the Windows ping program, which you will find in the TCP/IP program group. For full details refer to *Network Administrator's Reference Volume 1: Planning, Installation, and Configuration.*

Using the NBUTIL Program

Installing DOS LAN Services to run on TCPBEUI allows your computer to communicate with other computers that are also running TCPBEUI. TCPBEUI is an implementation of the Network Basic Input/Output System (NetBIOS), which is designed to operate with TCP/IP. This implementation adheres to the RFC 1001/1002 specification, allowing users to run NetBIOS applications over their TCP/IP networks. Both the client and the server must be running NetBIOS over TCP/IP to communicate.

When using TCPBEUI to communicate to other workstations across multiple subnets, you must use the NBUTIL.EXE utility. NBUTIL creates a local name cache on your workstation. NBUTIL associates IP addresses with NetBIOS names and stores this information so TCPBEUI can locate other workstations across subnets.

The NBUTIL program is accessed by using the DOS command NBUTIL with a variety of options that allow you to perform the following tasks:

- Add a NetBIOS name/IP address pair to the NetBIOS name table.
- Delete all entries from the NetBIOS name table.
- Display all the current entries in the NetBIOS name table.

The NBUTIL command must be executed after the TCP/IP protocol driver is running. Therefore, if you are using Windows for Workgroups, in which case the TCPPro VxD protocol driver will have been installed, you must run the NBUTIL command from a DOS prompt only.

Note: If you exit Windows, the protocol driver will be terminated and the NetBIOS name table is no longer in memory. You must re-enter the NBUTIL command after starting Windows.

If you are running Windows with DLS and you installed the TCPPro Real-mode Driver, you can also enter the NBUTIL command manually at the DOS prompt.

Note: If you restart your PC after specifying the command, the NetBIOS name table is no longer in memory and you must re-enter the command after restarting your PC.

If you want to run the command automatically each time your PC is started, enter the command in the AUTOEXEC.BAT file following the commands associated with loading the TCP Pro real mode protocol driver.

You can add the NBUTIL command to add entries to the NetBIOS name table in two different ways:

- By adding the IP address of each system you want to access with its associated NetBIOS name individually.
- By creating an ASCII text file containing a number of IP addresses with their associated names. All of these names can be added to the NetBIOS name table by invoking the NBUTIL command only once.

The following example demonstrates how to use NBUTIL to store information on a domain controller:

```
nbutil -a 129.35.15.136 tdomain -w

nbutil -a 129.35.15.136 tserver -x
```

where tdomain is the name of the domain and tserver is the name of the server.

NBUTIL Command Examples: The following command adds the NetBIOS name MailServer with the IP address 111.111.11.11 to the NetBIOS name table. (The LAN adapter number used by the TCP Pro protocol driver is 2.)

```
NBUTIL -a 111.111.11.11 MailServer -l 2
```

The following command clears the NetBIOS name table. (The LAN adapter number used by the TCPPro protocol driver is 2.)

```
NBUTIL -c -l 2
```

The following command translates the NetBIOS name FileServer into names that can be used by servers running LAN Manager and adds them to the NetBIOS name table. The IP address of FileServer is 111.111.11.11. The LAN adapter number used by the TCP Pro protocol driver is 1.

```
NBUTIL -a 111.111.11.11 FileServer -x -l 1
```

The following command adds the entries in the ASCII text file called NAMES1 to the NetBIOS name table and translates the NetBIOS names into names that can be used by servers running LAN Manager. The LAN adapter number used by the TCP Pro protocol driver is 0, therefore, the -1 option is not required.

```
NBUTIL -f NAMES -x
```

Note: If you are using TCP Pro for both LAN and remote access, there are two protocol drivers active. If you intend to use NetBIOS applications for both

connections, you must identify the LAN adapter number for each driver in separate NBUTIL commands.

For details of the syntax of the NBUTIL command please refer to *Network Administrator's Reference Volume 1: Planning, Installation, and Configuration.*

3.13 NETWORK.INI Configuration File Parameters

When DOS LAN Services is started using the NET START command, the parameters in the NETWORK.INI file are read and used to setup the behaviour of the DOS and Windows clients. A NETWORK.INI file was created because DOS truncates any commands that are more than 127 characters long; therefore it is not possible to pass all of the parameters to the NET START command.

The NETWORK.INI file resides in the directory where you installed DOS LAN Services. NETWORK.INI has the following main sections:

- Network
- Messenger
- Netpopup
- Peer

Note: There are also other sections that may appear in the NETWORK.INI as you configure your environment, such as Password Lists, Local Applications, and Network Applications.

You can change the NETWORK.INI file manually or by using the DOS LAN Services Setup program. The following tables provide information on parameters in the Network, Messenger, Netpopup and Peer sections.

NETWORK.INI Network Parameters

The following table provides details of the parameters in the [network] section of NETWORK.INI.

Note: All of the following parameters are valid for the virtual redirector except for autocache.

Table 11 (Page 1 of 3). NETWORK.INI Network Section Parameter Values

Parameter	Description	Valid Values	Default Value
computername	Identifies the workstation to the network	Up to 15 alphanumeric characters or special characters including ! # $ % & ( ) ¢ _ { } ^ ` ~	Name specified at installation
lanroot	Directory where DOS LAN Services is installed and starts	Fully qualified path (drive letter and path)	C:\NET
autologon	Prompts user to logon to a domain when DOS LAN Services starts	Yes, No	Yes
autostart	Indicates which services to start when NET START is entered	netbeui, basic, full, predir, messenger, netpopup, peer	Basic
guiconfig	Specifies color scheme to be used in DOS GUI		0,0,1

Table 11 (Page 2 of 3). NETWORK.INI Network Section Parameter Values

Parameter	Description	Valid Values	Default Value
username	Identifies the user to the network	Up to 20 alphanumeric characters or special characters including ! # $ % & ( ) ¢ _ { } ^ ` ~	Name specified at installation
domain	Name of the domain that the workstation belongs to	Up to 15 alphanumeric characters or special characters including ! # $ % & ( ) ¢ _ { } ^ ` ~	Name specified at installation
reconnect[4]	Specifies whether persistent connections are reconnected when logging on	Yes, No	Yes
lslogon	Specifies whether logon verification is to be performed by the domain controller	Yes, No	No
numbigbuf[1,2]	Specifies the number of big buffers to use (Full and Virtual redirectors only)	0 to 4096	2
sizebigbuf[1,2]	Specifies the size of big buffers in KB (Full and Virtual redirectors only)	4096 to 32768	4096
numworkbuf[1]	Specifies the number of work buffers to use	2 to 16	2
sizworkbuf[1]	Specifies the size of work buffers to use in KB	512 to 16384	1024
extraheap[1,2]	Allocates extra heap space for the redirector, and should be tuned for file-intensive applications, such as databases	1024 to 32768	0
keepcon	Specifies the time to keep dormant connections	0 to 65000	60
sesstimeout	Specifies the time to keep dormant sessions	10 to 30000	90
autocache[1]	Automatically allocates numbigbuf, sizbigbuf, and extraheap based on the amount of XMS memory available, overriding the individual values set for these parameters, and is recommended to increase performance	Yes, No	Yes
printbuftime[1]	Specifies the amount of time, in seconds, before a print job is sent to the server after the print job is submitted	0 to 65535	0
lanas[1]	Specifies the number of LAN adapter cards used by the workstation	0 to 7	1
ripl	Identifies a remote IPL workstation	Yes, No	No
passwordcaching	Indicates that passwords are to be cached to a file and saves passwords to servers in a password protected file so the user does not have to enter a password for each server that they access	Yes, No	Yes

Table 11 (Page 3 of 3). NETWORK.INI Network Section Parameter Values

Parameter	Description	Valid Values	Default Value
multilogon[5]	Indicates whether the user ID can be logged on at multiple workstations	Yes, No	Yes
securelogon[6]	Prevents local logon, if the user ID cannot be validated on the domain	Yes, No	No
browsealias[1,3]	Defines whether netnames or aliases are displayed when using the Browse option in a Windows environment	Yes, No	Yes
timesync[7]	Specifies whether or not the time on the local machine should be synchronized with the time at the domain controller at logon	Yes, No	Yes
biglie	Determines whether to lie about drives greater than 2GB (DOS does not support drives greater that 2GB; therefore it must lie if disks are greater than 2 GB)	Yes, No	Yes
mailslots[8]	Use mailslots	Yes, No	Yes
numdgrambuf[8]	Number of datagram buffers to be allocated	0 to 16	3
sbinterval[8]	Interval of time between sideband timeouts	0 to 65535	120
sbtimeout[8]	Time before timing out a sideband request	0 to 65535	3
sbcount[8]	Count before disabling sideband	0 to 65535	5

Notes:

1. This parameter must be manually added to the NETWORK.INI file to change the default. The installation program does not add this parameter to the NETWORK.INI file.
2. This parameter is overridden by autocache=yes.
3. Browsing for aliases is valid only on LAN Server domains. If this parameter is set to Yes, aliases are browsed. If no aliases exist on the domain, netnames are browsed automatically. If this parameter is set to No, browsing for aliases is not attempted.
4. While logon assignments are reestablished whenever you log on to the domain on which they exist, additional connections that you made to shared directories or printers, known as *persistent connections*, are also reestablished providing that you log on at the same workstation.
5. This parameter is valid only when both the user ID and the domain are 8 bytes or less in length.
6. This parameter is ignored if LSLOGON=NO.
7. If this parameter is not specified, DOS LAN Services synchronizes the time on the local machine with the time at the domain controller at logon. The length of time that it takes to log on will be reduced if timesync=no is added to the [network] section of NETWORK.INI; however, the time at the local machine will not be synchronized with the domain controller.
8. Not valid for the Basic redirector.

NETWORK.INI Messenger Parameters

The following table provides information on the parameters in the [messenger] section of NETWORK.INI.

Table 12. NETWORK.INI Messenger Section Parameter Values

Parameter	Description	Valid Values	Default Value
logfile	The name of the file where received messages are logged	Alphanumeric characters. See the DOS user's guide for valid characters that may be used when creating a file	MESSAGES.LOG
sizemembuf	Specifies the size of the message buffer to use in KB	512 to 4096	512
nummsgnames	Specifies the number of message names to be added to the workstation	2 to 8	2

NETWORK.INI Netpopup Parameter

The following table provides information on the [netpopup] section of NETWORK.INI.

Table 13. NETWORK.INI Netpopup Section Parameter Values

Parameter	Description	Valid Values	Default Value
msgtimeout	Defines the length of time, in seconds, that a message is displayed if Esc is not pressed, if the value is set to -1, a message is displayed until Esc is pressed.	-1 to 1800	60

NETWORK.INI Peer Parameters

The following table provides information on the [Peer] section of NETWORK.INI.

Attention

Whilst the following represents a complete list of parameters, certain parameters have been included which may not currently be relevant. In particular, parameters that imply multiple concurrent client connectivity to peer workstations are not implemented in this release of DOS LAN Services.

Table 14 (Page 1 of 3). NETWORK.INI Peer Section Parameter Values

Parameter	Description	Valid Values	Default Value
A20Moniter	Saves the state of the A20 line during task switching, some memory managers fail when set to 1, if your system hangs and are using a memory manager this should be set to 0	0, 1	1

Table 14 (Page 2 of 3). NETWORK.INI Peer Section Parameter Values

Parameter	Description	Valid Values	Default Value
NumRDRs	Specifies the number of workstations that can connect to resources on your workstation at one time	3 to 251	10
NumShares	Specifies the number of resources that may be shared on the peer workstation	2 to 256	10
NumReqBuf	Indicates the number of buffers the Peer will use to receive requests from clients and send responses to clients.	2 to 127	8
SizeReqBuf	Indicates the size (in bytes) of the buffer the peer uses to receive requests from clients and send responses to clients. This is an alias of XmitSize.	512 to 3276	4096
XmitSize	Specifies the size (in bytes) of the transmit buffers the Peer will use when transferring data (NumReqBuf * XmitSize < 48KB)	512 to 32768	2048
MaxShares	Indicates the maximum number of resources that may be shared on the peer workstation. This is an alias of numshares.	2 to 256	10
MaxConnections	Indicates the maximum number of connections clients can have to the peer workstation.	2 to 500	128
MaxCmds	Indicates the maximum number of NCBs (Network Control Blocks) that the peer can use.	4 to 255	12
MaxTx	Indicates the maximum number of rerequests that a peer workstation may process at one time.	1 to 8	4
Interval	Indicates the maximum period (in 50 millisecond units), from when the peer yields control, until the peer at background is awakened.	20 or greater	20
TaskTimeSlice	Specifies the amount of time (ticks) the foreground/background will each run. (Timeslice=FB) **Value** **Ticks** 0 2 1 4 2 6 3 10 4 14 5 22 6 30 7 42 8 56 9 72	00 to 99	54

Table 14 (Page 3 of 3). NETWORK.INI Peer Section Parameter Values

Parameter	Description	Valid Values	Default Value
OpenMode	Indicates the mode in which files will be opened when an open request is received 0 = Use Open mode that application requests 1 = DENY-NONE sharing mode if read-only access to .EXE or .COM files. COMPATIBILITY-MODE for .BAT files or if write access to .EXE or .COM files. 2 = DENY-NONE sharing mode if read-only access to .EXE or .COM files. DENY-WRITE sharing mode if read-only access to .BAT files. COMPATIBILITY-MODE if write access to .EXE, .COM or .BAT files. 3 = DENY-NONE sharing mode on all compatibility mode opens	0 to 3	3
FileShareSize	Specifies the number of bytes allocated for the DOS storage area used to record file sharing information, (If SHARE.EXE is started before the Peer, the values that were specified when SHARE.EXE was started will be used)	512 to 32768	2048
ShareLocks	Specifies the maximum number of active locked ranges in files that you can share with the Peer service, (If SHARE.EXE is started before the Peer, the values that were specified when SHARE.EXE was started will be used)	20 to 1000	20
FMShare[1]	Indicates whether you want to be able to share directories from the Windows file manager	Yes, No	Yes
SpoolDir[1]	Indicates where you want your spool files to be stored, this allows you to store your spool files somewhere other than the DOS LAN Services program directory, RIPL machines need to have this parameter to share printers when using the Peer service	Any local drive and directory	C:\NET

Notes:

1. This parameter must be manually added to the NETWORK.INI file to change the default. The installation program does not add this parameter to the NETWORK.INI file.

Sample NETWORK.INI File

The following is a sample NETWORK.INI file.

```
[network]
guiconfig=1,0,1
computername=W4602R10
lanroot=C:\NET
autostart=netbeui predir peer messenger netpopup
username=A948R1
domain=ITSCAUS
lslogon=yes
reconnect=no
passwordcaching=yes
timesync=no
multilogon=no

[Messenger]
sizemembuf=1024

[netpopup]
msgtimeout=15

[install]
peer=yes
gui=yes
windows=yes
protocol=netbeui

[Password Lists]
USERID=C:\NET\USERID.PWL
A948R1=C:\NET\A948R1.PWL

[peer]
fmshare=yes
```

Figure 85. Sample DOS LAN Services NETWORK.INI File

3.14 Password Coordination

The Network SignON Coordinator Client provides the end user a way to perform a signon/signoff operation. The Client can operate on either an OS/2 or DOS platform and manage passwords and logons in:

- OS/2 Warp Server Domains
- NetWare Servers
- Hosts
- Local facilities

These operations are specified in a user configured ASCII file (NSC.INI) which contains the location definitions which may contain a user ID to be used for request processing. The same location can be defined as many times as is necessary to include all the user IDs that you have at that location.

Network SignON Coordinator will prompt you for your current password and user ID (if not already specified in NSC.INI) which is then combined with location information to process your request (as shown in Figure 86 on page 117).

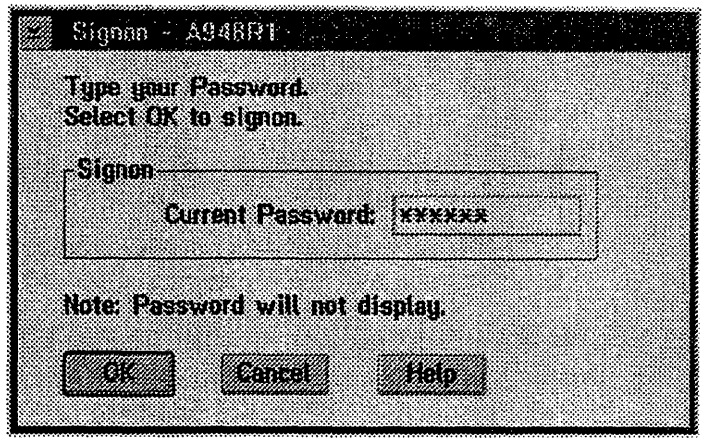


Figure 86. Network SignON Coordinator - Signon Window

Options that can be used in NSC are:

- Use a different user ID than the one the end user inputs.
- Specify that the user is to be logged on to a specific domain.
- Specify an Exit Routine to be executed after Network SignON Coordinator performs the signon/signoff operation. Network SignON Coordinator allows a user to signoff all locations with a single command.
- Change password across all defined domains in one operation. If the user selects the option to change passwords, the user is prompted to enter and confirm the new password as Figure 87 illustrates. The password change is then initiated at all locations defined in their Network SignON Coordinator configuration file.

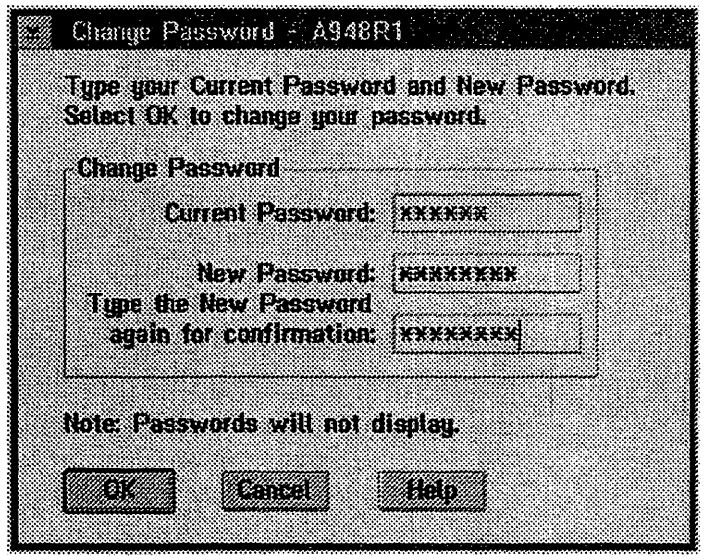


Figure 87. Network SignON Coordinator - Change Password Window

Network SignON Coordinator provides additional functions and options to allow users to tailor the system to fit their needs. These functions and options include:

- Queueing requests to LAN Server domain controllers when they are not available.

- The ability to specify different user IDs on each system while using the same signon password on every system.
- An OS/2 API and toolkit that supports all of the functions of Network SignON Coordinator while bypassing the user interface.
- User Exits for additional coordination or synchronization of signons, changing passwords and signoffs.
- Configuration options for user ID character set, minimum/maximum user ID length, and minimum/maximum password length.

To summarize, Network SignON Coordinator is a tool for end users who, by entering their user ID and password once at a menu, have their signon requests processed at any number of OS/2 Warp Server domain controllers.

Note: Users in a double-byte character set (DBCS) environment are limited to using single-byte characters in their user IDs and passwords.

Security Considerations

Network SignON Coordinator is not a security product; it is a productivity aid. However, since it does help the user manage passwords, some care has been taken to avoid creating additional security exposures for the user.

> **Attention**
>
> Review the following with respect to your security requirements. If any of these possible exposures is unacceptable, you should not use Network SignON Coordinator.

- Network SignON Coordinator assumes the user has the same password at all locations. If a user's password is compromised, the security exposure may be greater since all locations can be accessed with that password.
- Network SignON Coordinator can remember the user's password once it has been entered, but only if the SAVEPW option is configured. The default operation requires the user to reenter the password each time it is required.

  The password is always discarded when Network SignON Coordinator is terminated, even if SAVEPW is configured.
- Network SignON Coordinator does not keep passwords in the clear in memory except when necessary to call external application programming interfaces. The password is masked and distributed using a simple reversible algorithm designed to prevent casual viewing of the password.
- Network SignON Coordinator does not send passwords from Network SignON Coordinator Clients to Network SignON Coordinator Servers in the clear. The password is masked to prevent casual viewing of the password via network analyzers.
- Products supported by Network SignON Coordinator send the passwords across the network using different techniques. For information on how passwords are communicated by these products, consult the product information for that product.
- Network SignON Coordinator provides no function for restricting access to locations. Access to other locations is controlled by each location's own security facility.

- Network SignON Coordinator performs no encryption, and is therefore not subject to any export restriction related to encryption.

Installation

OS/2 Warp Server installs the OS/2 Client and Server part of Network SignON Coordinator. This allows a workstation to function as both a Network SignON Coordinator OS/2 Client and a Network SignON Coordinator Server.

Configuration

All configuration information for Network SignON Coordinator itself is stored in a flat ASCII file called NSC.INI. An ASCII file editor can be used to modify the file to customize the configuration. The NSC.INI file comes with the defaults for menu interaction. Configurable entries include:

- Minimum and maximum user ID
- Password lengths
- Sound
- Menu shortcut
- Default user ID

The NSC.INI file does not come with any pre-configured LAN Domain Server or Host names. Entries for each LAN Server and host must be added. The default NSC.INI file for an OS/2 client only contains the following line:

```
LOCAL,ON
```

The NSC.INI file may be replicated to multiple directories to allow support of different users or different system views. A copy of the file must either reside in the current directory or in a directory specified in the DPATH when executing NSC, NSCRSON, NSCRSOFF or calling the NSCRSIGN API.

The NSC.INI file may be modified by any ASCII file editor (for example, the OS/2 Enhanced Editor). Each line defines a configuration option or operation. Any line beginning with an asterisk is considered to be a comment and is ignored. Any text following the first blank (space) character on a line is considered to be comment text and is ignored. Although options are all shown in upper case, they may be entered in upper, lower or mixed case.

An example of a configuration file is shown in Figure 88.

```
USERID=A948R1
EXIT,ID=1,NAME=D:\NSC\PEERPASS.CMD
LOCAL,ON,EXITID=1
LANSERVER,IBM,NAME=W4602S01,ON
LANSERVER,NOVELL,NAME=NW312,USERID=NWUSER
```

Figure 88. OS/2 Client NSC.INI File Example

```
@ECHO OFF
rem %1 = 0 for signon, 1 for signoff, 2 for change password,
rem %2 = Configuration definition index
rem %3 = Return code
rem %4 = User ID
rem %5 = Current Password
rem %6 = New Password
rem
rem exit if not a change password request
IF NOT %1 == 2 GOTO END
rem repeat the NET PASSWORD line with the name of all the peers that
rem you want to change your password on
NET PASSWORD \\W4602R01 %4 %5 %6
NET PASSWORD \\PEERCD %4 %5 %6
:END
```

Figure 89. NSC Exit for Changing Peer Passwords

The example allows a logon to an OS/2 Warp Server domain, and defines user IDs on two IBM Peer for OS/2 Version 1.0 machines that are to be maintained. The NSC Exit PEERPASS.CMD allows passwords to be changed on peer workstations.

The following table provides details of the NSC.INI options that may be set.

Table 15 (Page 1 of 2). NSC.INI Configuration File Options

Option	Description	Valid Range	Default Value
USERID[1]	Specifies the user ID to be used for signon operations	Any character that is part of the user ID Character Set	none
CHARSET[2]	Specifies characters (other than alphanumerics) that are valid in user IDs and passwords	Graphic ASCII characters, other than a space	All alphanumeric characters plus the non-alphanumeric characters #, @ and $
MINUIDLEN	Defines the minimum user ID length	1 to 8 characters	4 characters
MAXUIDLEN	Defines the maximum user ID length	1 to 47 characters	8 characters
MINPWLEN	Defines the minimum password length	1 to 8 characters	5 characters
MAXPWLEN	Defines the maximum password length	1 to 8 characters	8 characters
BEEP	The BEEP option allows the user to turn on or off the beeps that are sounded when error messages are displayed or invalid keys are pressed	ON, OFF	ON
SIGNON[3]	Causes the Signon dialog to immediately be displayed when the PM interface (NSC.EXE) is started	none	none

Table 15 (Page 2 of 2). NSC.INI Configuration File Options

Option	Description	Valid Range	Default Value
SAVEPW[4]	Specifies that the end user's password should be recorded and used for subsequent password requests in this session	ON, OFF	OFF
CONFIRMEXIT	Defines whether a warning message is displayed before Network SignON Coordinator exits	ON, OFF	OFF
DEBUG[5]	Specifies that additional information should be logged when a problem occurs	none	none

Notes:

1. Lower case alphabetic characters in the default user ID will be converted to upper case (see User ID Character Set Option). The user ID entered in the Network SignON Coordinator Signon menu becomes the default user ID for each system specified with a DOMAIN, HOST or LOCAL operations. This user ID may be overridden in any of these operations by specifying the USERID parameter for the operation.
2. This option is useful when you use the UPMCSET /E command to extend the user ID character set. You cannot specify the alphanumeric characters A through Z, a through z, and 0 through 9. Only graphic ASCII characters other than a space can be specified. (they are 0x21..0x7E, 0x80..0xFE). Lower case extended ASCII characters should be avoided, as they will not be converted to upper case, and may thus not give the desired result when passed to UPM or LAN. You can specify up to 159 characters. This is enough to specify all the non-alphanumeric graphic ASCII characters. No check is made for duplicate characters.
3. When specified the equivalent action of using the mouse to select *Actions*, *Signon*, and *Default Systems* is performed.
4. If you select the Default Signons or Change Password actions, the previously entered password is used. The password is not stored on disk, but hidden and masked in memory. When Network SignON Coordinator is closed, the saved password is no longer available.
5. This option should only be specified for problem determination purposes since user request processing is slower with this option defined.

The following is a list of the configuration and signon operation options defined in the configuration file.

Definition	**To specify**
LOCAL	UPM Local signon
NODE	UPM Node signon
LANSERVER	OS/2 Warp Server or NetWare Server logon
HOST	Host signon
SERVER	NSC/2 Server machine

The order of the operations is very important since Network SignON Coordinator executes them in order. The server definitions are also stored in the configuration file. Their position in the file relative to the signon operations determines where the signon operations are executed.

Using Password Coordination

From an OS/2 Warp Server workstation, or an OS/2 or DOS client workstation, a user can perform:

- Local logons - For administration of local UPM and logon to other applications like DB2/2
- LAN logon - Used by OS/2 Warp Server for attaching to a domain
- NetWare login - Used to log in to a NetWare Server
- Peer password management - managing your passwords on OS/2 peer workstations

Network SignON Coordinator uses two signon operations parameters in NSC.INI:

- LOCAL - for local logons and password changes in the local UPM
- LANSERVER - for one LAN (domain) logon and password changes

  LANSERVER is also used for NetWare server logins and password changes

  Password changes on OS/2 peer workstations are handled by a NSC exit which runs NET PASSWORD commands to change peer passwords.

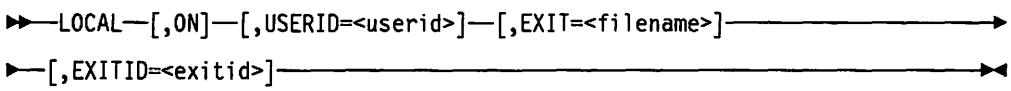
Note

IBM Peer for OS/2 Version 1.0 (for OS/2 Warp Connect clients) workstations do not support logons, however it still possible to maintain client passwords defined in the peer server because Network SignON Coordinator can use the NET PASSWORD command to perform password changes which only requires UPM on the peer workstation.

Network SignON Coordinator used in a pure peer environment is useful to synchronize passwords, not for logging on.

LOCAL Signon Operation

A LOCAL operation is used to make OS/2 UPM password changes and optionally logon to the local UPM. The syntax is:



The ON option requests Network SignON Coordinator to perform a local logon as well as synchronize password changes with UPM.

If the user's account on the local workstation is under a different user ID than the user ID provided to Network SignON Coordinator (from the USERID configuration option, from the command line, from the API, or from the Signon dialog), the USERID= parameter may optionally be specified. Lower case alphabetic characters in the user ID will be converted to upper case. This parameter also allows a user to synchronize passwords for multiple accounts on the client workstation, each with a different USERID= parameter.

If the EXIT parameter is optionally provided, Network SignON Coordinator will execute the specified command file or executable program for each request made for this Local operation. A complete path (up to 80 characters) may be specified if the command file or executable program is not in the PATH.

For example, the NSC OS/2 Client will perform a local logon for the user at signon and change the password on the client workstation when requested and execute the user command file PEERPASS.CMD after each request with the following operation:

```
LOCAL,ON,EXIT=D:\NSC\PEERPASS.CMD
```

```
@ECHO OFF
rem %1 = 0 for signon, 1 for signoff, 2 for change password,
rem %2 = Configuration definition index
rem %3 = Return code
rem %4 = User ID
rem %5 = Current Password
rem %6 = New Password
rem
rem exit if not a change password request
IF NOT %1 == 2 GOTO END
rem repeat the NET PASSWORD line with the name of all the peers that
rem you want to change your password on
NET PASSWORD \\W4602R01 %4 %5 %6
NET PASSWORD \\PEERCD %4 %5 %6
:END
```

Figure 90. NSC Exit for Changing Peer Passwords

Multiple requests for password change operations or any other operation can be defined within the configuration file to be executed either on the Client or at the Server. The EXIT parameter is required for password maintenance of peer workstations. Using NSC, peer workstations must have the same user ID defined as the user ID defined locally.

LANSERVER Signon Operation

A LANSERVER operation is used to make LAN Server password changes and optionally logon to the LAN Server. You can specify multiple LAN Server definitions to be processed locally, but LANSERVER definitions cannot follow a SERVER definition. The syntax is:

```
►►—LANSERVER,—[IBM | NOVELL],—[,NAME=<name>]—[,ON]—[,USERID=<userid>]—►
►—[,EXIT=<filename>]—[,EXITID=<exitid>]————————————————————————————►◄
```

The ON option requests Network SignON Coordinator to perform a logon to an OS/2 Warp Server Domain Controller or NetWare server as well as synchronize password changes.

The value of name is the OS/2 Warp Server domain or NetWare file server's name.

If the user's account on the server is under a different user ID than the user ID provided to Network SignON Coordinator (from the USERID configuration option, from the command line, from the API, or from the Signon dialog), the USERID parameter may optionally be specified. The user ID on a peer must be the same as the user ID defined locally. Lower case alphabetic characters in the user ID will be converted to upper case. This parameter also allows a user to synchronize passwords for multiple accounts on the same domain controller by

including multiple LANSERVER operations for the same domain controller, each with a different USERID parameter.

If the EXIT parameter is provided, Network SignON Coordinator will execute the specified command file or executable program for each request made for this LANSERVER operation. For example, an exit routine could check for a successful domain logon and perform a NET USE for a resource controlled by the domain. A complete path (up to 80 characters) may be specified if the command file or executable program is not in the PATH.

For example, the Network SignON Coordinator OS/2 Client will perform a LAN Server logon for the user on to domain `W4602D01` at signon and change the password on domain `W4602D01` when requested with the following operation:

```
LANSERVER,NAME=W4602D01,ON
```

Note: Lower case alphabetic characters in the domain name will be converted to upper case.

Note: Multiple LANSERVER operations can be specified, however they can only be executed from the Client. Since it is only possible to have one active domain logon and one active NetWare login on a workstation, only the primary domain and/or NetWare server should include the ON option. LANSERVER operations cannot follow a SERVER definition.

Figure 91 shows the Network SignON Coordinator main folder which is accessed from the OS/2 System folder.

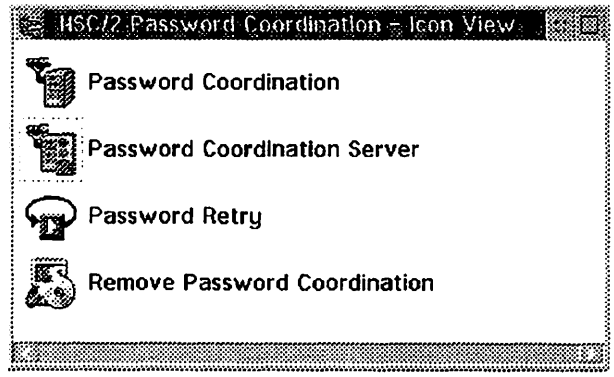


Figure 91. Password Coordination - Main Folder

For more information open *NSC Reference* and the *LAN Requester User's Guide* online book files.

Chapter 4. Adapter and Protocol Services

OS/2 Warp Server provides you with a wide range of supported networking protocols and communication adapters which you may use in many combinations to suit your requirements for a server system. Adapter and Protocol Services may be called the *communications engine* of OS/2 Warp Server since they provide communication support for any of the other components of this product.

To go even further, Adapter and Protocol Services also provide LAN support for applications that you may want to install on top of OS/2 Warp Server and for DOS and Windows applications that you can also run under OS/2.

This chapter will introduce Adapter and Protocol Services to you and explain how to install and configure it, and how to make use of the new and advanced features of this key component of OS/2 Warp Server.

4.1 Overview of Adapter and Protocol Services

In order to support the variety of network applications and services that come with OS/2 Warp Server, and to support many additional networking products, Adapter and Protocol Services provide a very complete set of networking protocols which can be used in a LAN environment as well as for wide area networking.

New Features

Before going into the details of Adapter and Protocol Services, we want to highlight the new features that are provided with OS/2 Warp Server in regard to networking support:

Table 16. New Features of Adapter and Protocol Services

System Component	Description
Dynamic Host Configuration Protocol (DHCP) client	DHCP clients will contact DHCP servers on the network in order to automatically and dynamically obtain the addresses and configuration information about the network and about host operational parameters as specified by network administrators.
Dynamic Domain Name Services (DDNS) client	DDNS enhancements enable client hosts to dynamically register their name and address mappings in the DNS tables directly, rather than having an administrator manually perform the updates.
Support for 1000 clients with TCPBEUI	The NetBIOS over TCP/IP interface can now be activated four times which will allow for 1000 active NetBIOS sessions that your OS/2 Warp Server system can support over TCP/IP at the same time.

We will discuss those features in separate chapters later in Chapter 5, "TCP/IP Services" on page 167 and Chapter 6, "NetBIOS over TCP/IP (TCPBEUI)" on

© Copyright IBM Corp. 1996

page 259. In this chapter we will discuss the base MPTS functions and some enhancements.

Adapter and Protocol Services can be divided into two parts,

- Actual adapter and protocol support (LAPS)
- Sockets multiprotocol transport services (MPTS)

Adapter and Protocol Support (LAPS)

Originally, LAPS was called LAN Adapter and Protocol Support, but since it now also includes drivers for wide area networking adapters, we skipped the word LAN, but kept the familiar acronym LAPS. LAPS includes the following networking protocols based on the Network Driver Interface Specification (NDIS) standard:

- NetBIOS
- TCP/IP
- IEEE 802.2
- IPX/SPX over NDIS support
- NetBIOS over TCP/IP
- NetBIOS over IPX support

With LAPS, you will also have virtual IEEE 802.2 and NetBIOS support for DOS and Windows application running on your OS/2 Warp Server system.

A wide range of LAN adapters for token-ring, Ethernet and FDDI are included as well as WAN adapters and serial and parallel communications support for NDIS. A complete list of adapters supported by Adapter and Protocol Services can be found in the \IBMCOM\MACS\READMAC.TXT file. Figure 92 on page 127 shows an overview of the LAPS component of Adapter and Protocol Services.

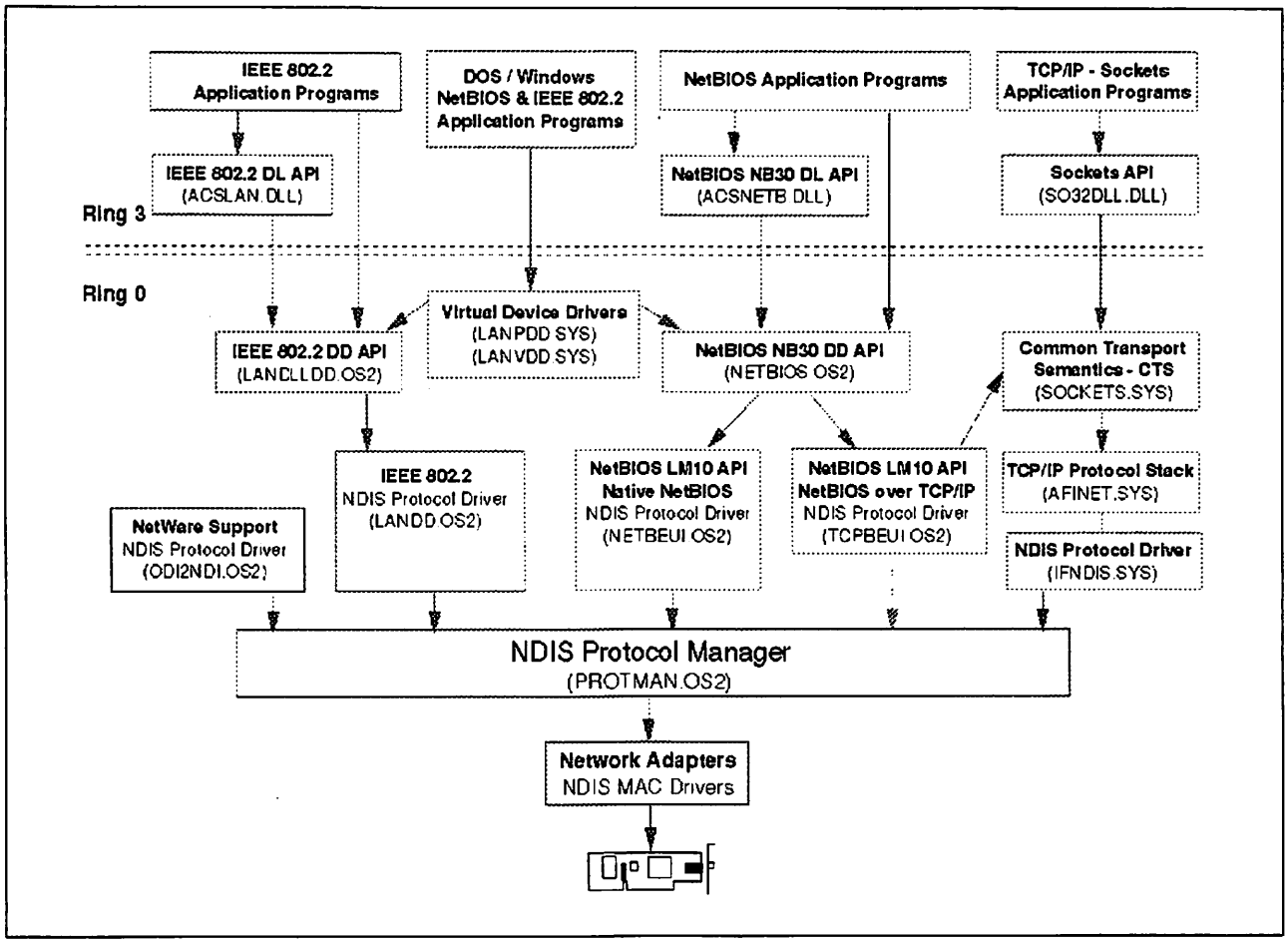


Figure 92. LAN Adapter and Protocol Support (LAPS) Overview

Note: Virtual TCP/IP support for DOS and Windows applications is also provided with OS/2 Warp Server, but that is included in TCP/IP Services. Please see Chapter 5, "TCP/IP Services" on page 167 for more information on that topic.

Note: Virtual NetWare IPX and SPX support for DOS and Windows applications is also provided with OS/2 Warp Server, but that is part of the NetWare Requester for OS/2. Please see 4.5, "NetWare Requester for OS/2" on page 157 for more information on that topic.

The files that make up LAPS and its configuration are placed under the \IBMCOM directory tree on the OS/2 boot drive.

Network Driver Interface Specification (NDIS)

IBM's transport strategy is based on the Network Driver Interface Specification (NDIS) - a standard jointly developed by 3COM and Microsoft Corporation. NDIS allows different network protocols to operate over the same LAN interface at the same time.

NDIS is a standardized Medium Access Control (MAC) interface for network adapter drivers and protocol drivers. It has become a de facto industry standard, providing a common, open interface that enables different manufacturers of network adapters and LAN software developers to produce products which communicate with each other.

NDIS separates protocol handling from hardware manipulation by defining functions that protocol drivers and network adapter drivers must provide to each other.

NDIS defines:

- Specifications for network protocol drivers
- Specifications for network adapter drivers
- Interface between the above two layers
- Binding process to link these protocol and adapter drivers

A *network protocol driver* provides the communication between an application and a network adapter driver.

A *network adapter driver*, or MAC driver, provides the communication between a network adapter and a protocol. The main function of the network adapter driver is to support network packet reception and transmission.

Each driver has an upper and a lower boundary. The drivers are linked together to form a stack by binding the lower boundary of one driver to the upper boundary of another driver. The MAC driver at the bottom of the stack always has its lower boundary connected to the physical layer - the network adapter hardware.

The NDIS specification defines the binding process of the drivers. Three components are used to form and manage the protocol stack from individual drivers. These are:

PROTOCOL.INI

An ASCII file that defines the protocol drivers and adapter drivers in use and their binding information.

PROTMAN.OS2

A Protocol Manager.

NETBIND.EXE

Initiates the final binding process.

The LAPS component of Adapter and Protocol Services contains the above three files, the protocol and adapter drivers and a utility for easy installation and configuration of the required drivers. LAPS also contains *Virtual Device Drivers* which make the installed protocols available to DOS and Windows sessions under OS/2, without the need for specific DOS protocol drivers.

Figure 93 on page 129 provides an illustration of an NDIS protocol stack in comparison to both the OSI reference model and the IEEE model.

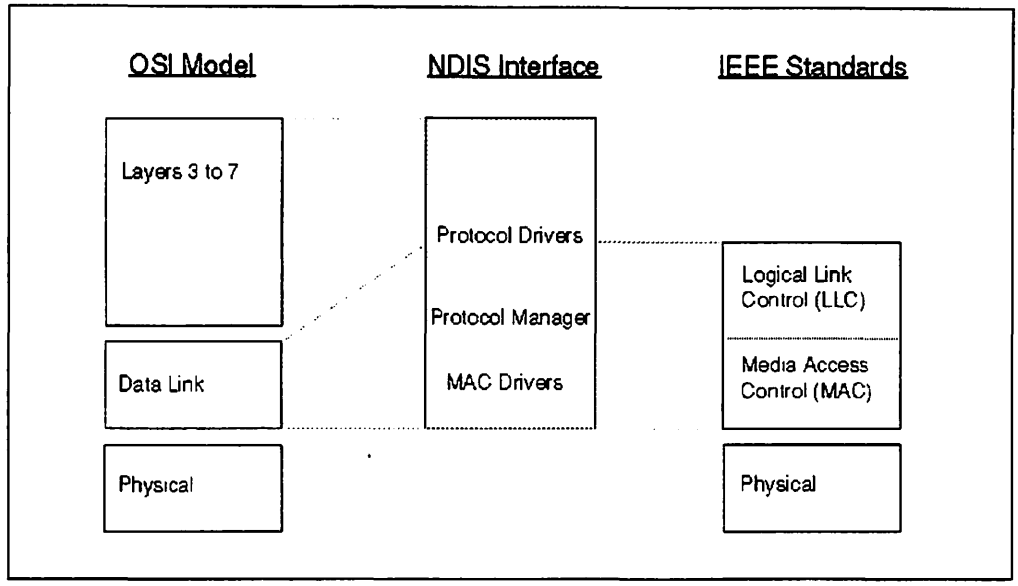


Figure 93. NDIS, OSI and IEEE Comparison

Multiple Protocol Support

NDIS allows multiple protocols to be bound to a single MAC driver - that is, to share a network adapter. Figure 94 shows the NDIS protocol stacks when NetBIOS, IEEE 802.2 and TCP/IP are loaded together. In this example, two LAN adapters are in use. NetBIOS and IEEE 802.2 are bound to one of the adapters, and the other adapter is dedicated to the TCP/IP protocol (although there is no reason why all three protocols could not have been bound to both adapters). The configuration information defining which protocol(s) is bound to which adapter(s) is contained in the PROTOCOL.INI file.

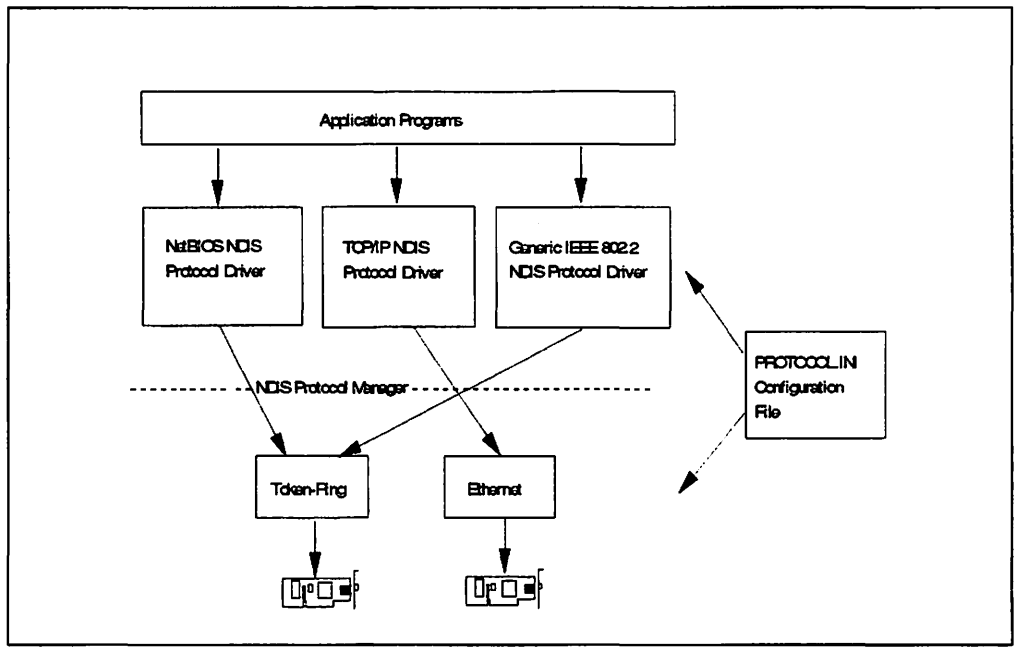


Figure 94. NDIS - Multiple Protocols

PROTOCOL.INI

PROTOCOL.INI contains the NDIS configuration information for network adapter drivers and protocol drivers for a workstation. PROTOCOL.INI is an ASCII file that can be edited manually, but this is generally not recommended. We recommend that you always use the Adapter and Protocol Services configuration utility to ensure the creation of valid PROTOCOL.INI and CONFIG.SYS files. Please refer to 4.3, "Additional Configuration for Adapter and Protocol Services" on page 142 on more information on how to use the configuration utility.

The PROTOCOL.INI file consists of four sections:

- Protocol Manager
- Configuration
- Protocol drivers
- MAC (network adapter) drivers

All these sections have the following structure:

```
[module name]
  parameter=value
```

The following is an example of a PROTOCOL.INI file configured with both NetBIOS and TCP/IP protocol stacks (similar to Figure 94 on page 129). The first entry is the protocol manager, which is the driver that controls the binding process.

```
[PROT_MAN]

   DRIVERNAME = PROTMAN$
```

The configuration section defines which protocols are used and what types of adapters are configured. In the following example, `netbeui_nif` and `tcpbeui_nif` are the protocol drivers, and `IBMTOK_nif` is the adapter configuration (in this case an IBM Token-Ring adapter).

```
[IBMLXCFG]

   netbeui_nif = netbeui.nif
   tcpip_nif = tcpip.nif
   IBMTOK_nif = IBMTOK.NIF
```

The `Bindings=` statements under the various protocol drivers specifies the module name of the MAC driver to which the protocol driver will bind to form a protocol stack or stacks. In this example, NetBIOS, the NetBIOS API is using the NetBEUI protocol driver, which itself is bound to the token-ring MAC driver. TCP/IP is also bound to the token-ring MAC driver.

```
[NETBIOS]

   DriverName = netbios$
   ADAPTER0 = netbeui$,0

[netbeui_nif]

   DriverName = netbeui$
   Bindings = IBMTOK_nif

[tcpip_nif]
```

```
   DriverName = TCPIP$
   Bindings = IBMTOK_nif

[IBMTOK_nif]

   DriverName = IBMTOK$
```

More statements of the kind of `parameter=value` may appear under each protocol and MAC section. The meanings of `parameter` and the allowed ranges and types for `value` are contained in network information (.NIF) files which exist for each protocol and MAC driver. The configuration program parses those NIF files to check what can be configured for any given section in PROTOCOL.INI and if a configuration item is valid. If no additional parameters are specified in the PROTOCOL.INI sections, default values will be used as defined in the .NIF files.

NDIS NETBIND Process

When a workstation is initialized, the following process takes place:

1. The Protocol Manager is the first NDIS-related driver to be initialized during the CONFIG.SYS process. During initialization, the Protocol Manager reads the PROTOCOL.INI file.
2. The information in PROTOCOL.INI is parsed into an image table that is accessible to other NDIS drivers.
3. As CONFIG.SYS processing continues, other drivers are loaded. As each is initialized, the related information in the image table is read. The NDIS driver then registers with the Protocol Manager.

   After all drivers and protocols are processed, the Protocol Manager has a list of active NDIS drivers and their desired bindings.
4. A NETBIND is issued, and the desired bindings take place.

Socket/Multiprotocol Transport Services (MPTS)

The Sockets interface allows you to develop distributed or client/server applications using various transport protocols. The application can select the transport protocol or request that the Socket/MPTS layer determine the protocol. Most socket applications available today communicate with either TCP or UDP.

Sockets are duplex, which means that data can be transmitted and received simultaneously. Sockets allow you to send to, and receive from, the socket as if you are writing to and reading from any other network device.

Socket/MPTS provides the support for three kinds of address families for the Sockets application programming interface (API):

1. TCP/IP address family (AF_INET)
2. NetBIOS address family (AF_NB)
3. OS/2 address family (AF_OS2)

It also provides a local IPC transport for Sockets applications (inter-process communications support that does not issue any calls to the network).

Figure 95 on page 132 shows an overview of Socket/MPTS.

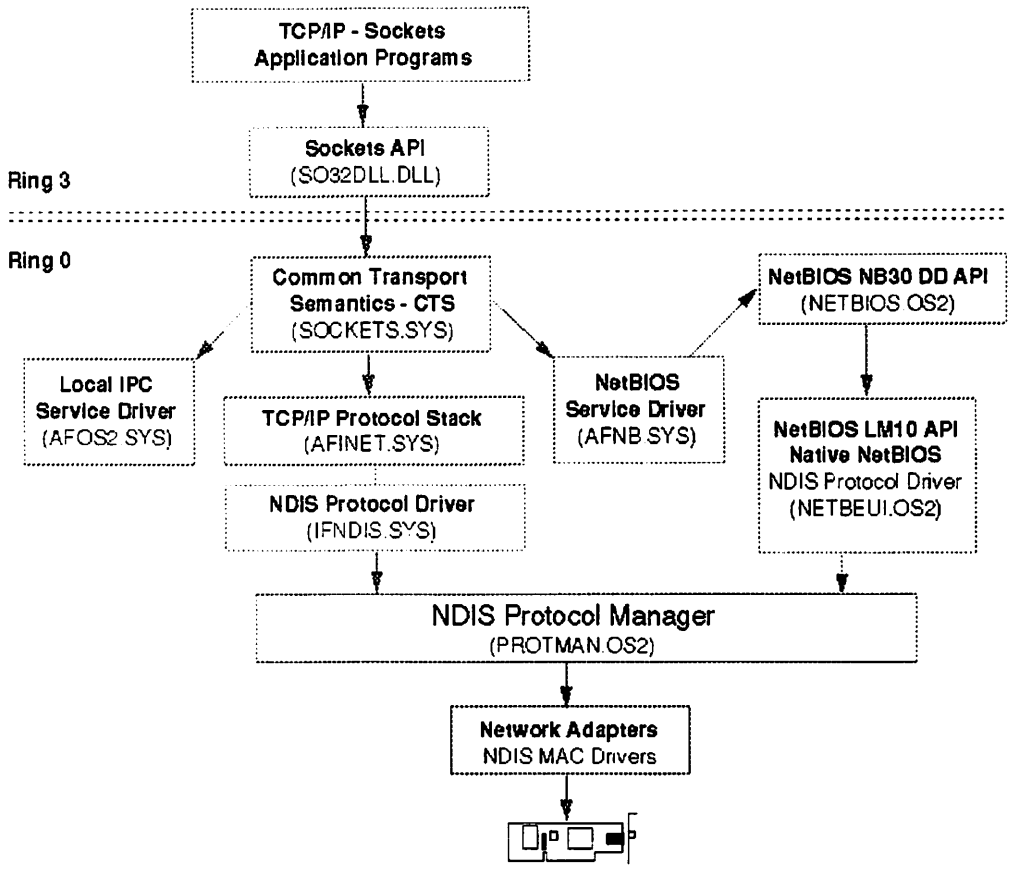


Figure 95. Socket/MPTS Overview

As you can see from comparing Figure 92 on page 127 and Figure 95, the LAPS and MPTS components overlap on the TCP/IP Sockets support and protocol stack. Whereas LAPS merely allows the TCP/IP protocol to be added to an adapter configuration, MPTS allows the user to select and configure the appropriate Sockets support, and it also contains the files that make up Sockets and TCP/IP in the bsl.MPTN directory tree on the OS/2 boot drive.

If a Sockets application has been coded to use a certain address family, it would normally be bound to the transport protocol that this address family supports. That is, for example, an application using the AF_INET address family would also use TCP/IP as its transport protocol. This is called *native* transport.

If you need to run that application over a different transport, and there were only support for native transport, you would have to rewrite the application to use the address family that is native to the other transport protocol. With the Multiprotocol Transport Network (MPTN) architecture and the AnyNet product family, however, IBM introduces the capability of *non-native* networking. That means that an application can use any transport network, even if that transport is not natively supported by the application. In that case, the above program, which has been coded to use the AF_INET address family, could use, for instance, the NetBIOS protocol without having to be re-written to use the AF_NB address family.

Using Socket/MPTS on its own allows ONLY native networking of Sockets applications (AF_INET over TCP/IP, AF_NB over NetBIOS, AF_OS2 over local IPC). However, this release of MPTS, also known as the *Converged Stack*, allows

coexistence with the IBM AnyNet/2 product. AnyNet/2 also introduces an SNA services driver, which means that running TCP/IP applications over SNA or NetBIOS applications over SNA is also made possible. For more details about AnyNet/2 and non-native Sockets, please refer to *Inside OS/2 Warp Server, Volume 2: Using SystemView, Backup/Recovery and Advanced Print* which is planned to be available in May 1996.

4.2 Installing Adapter and Protocol Services

As this component of OS/2 Warp Server provides communication support to all other parts of the product, it will always be installed when you install an OS/2 Warp Server system. Therefore, it cannot be explicitly selected on the OS/2 Warp Server Setup and Installation Menu.

Note: If you are installing OS/2 Warp Server remotely in unattended mode (response file installation method using CID), then you must include the Adapter and Protocol Services component in the installation procedures. Otherwise, your system will not be working, apart from base OS/2.

Adapter and Protocol Services will attempt to detect and identify any LAN adapters that are installed in your system. See the \IBMCOM\MACS\READMAC.TXT file for a list of adapter drivers which are supplied with OS/2 Warp Server. However, only the first adapter that could be found will be automatically included in the configuration. You may add more adapters, and you may add additional adapter drivers which are not included in OS/2 Warp Server, which we will show later.

As far as network protocols are concerned, the initial configuration of Adapter and Protocol Services depends on the features which you have selected to be installed. The following explains how each protocol is automatically installed:

- The IBM NetBIOS protocol will be automatically configured if any of the following components are selected:
  - File and Print Sharing Services
  - Remote Access Services
  - Systems Management Services with NetBIOS protocol enabled
  - Software Backup and Recovery Services with LAN backup option selected
- The IBM TCP/IP protocol will be automatically configured if any of the following components are selected:
  - TCP/IP Services
  - Systems Management Services with TCP/IP protocol enabled
  - Advanced Printing Services with TCP/IP printing option selected
- The NetWare Requester Support driver will be automatically configured if any of the following components are selected:
  - File and Print Sharing Services with NetWare File Sharing Gateway feature
  - Systems Management Services with IPX protocol enabled
- The IEEE 802.2 protocol will always be automatically configured.

Figure 96 on page 134 shows the OS/2 Warp Server Configuration menu with a possible initial configuration for Adapter and Protocol Services:

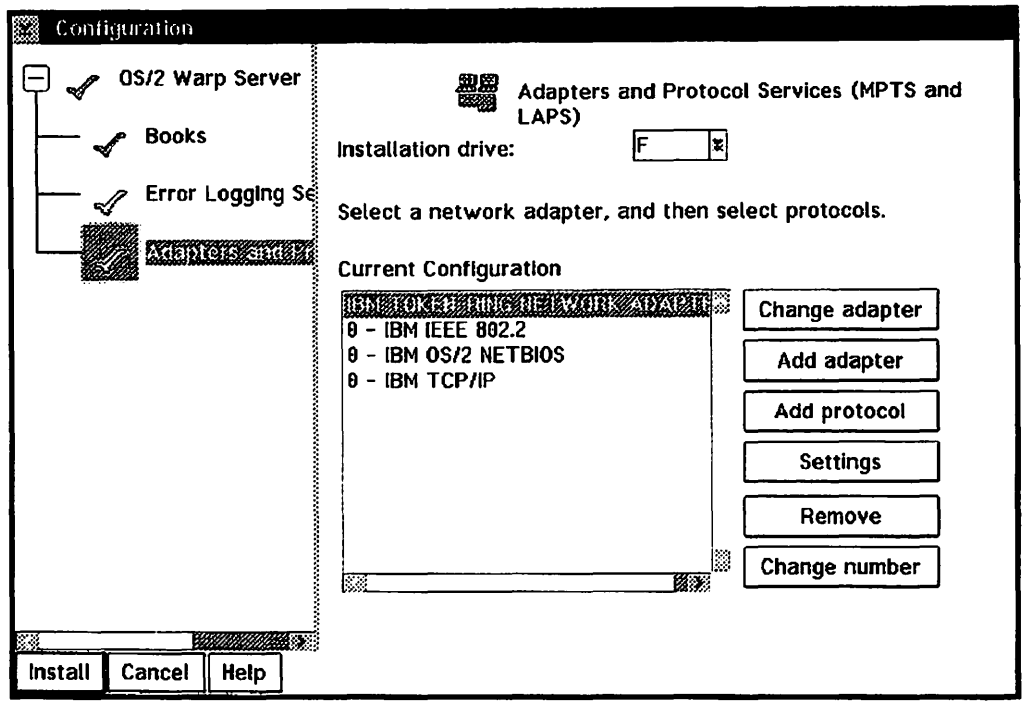


Figure 96. Initial Adapter and Protocol Services Configuration

The following table summarizes the configuration parameters of this page and describes their purposes.

Table 17 (Page 1 of 2). Adapter and Protocol Services Installation

Configuration Item	Configuration Data
Change adapter	Press this button if you want to change a network adapter for the current configuration. This may be necessary if the installation program could not detect your adapter configuration properly.
Add adapter	Press this button if you: 1. Want to add an adapter to your configuration 2. Want to add a new adapter driver which is not supplied with Adapter and Protocol Services This will bring up the menu that is shown in Figure 97 on page 135.
Add protocol	Press this button if you: 1. Want to add a protocol to your configuration 2. Want to add a new protocol driver which is not supplied with Adapter and Protocol Services This will bring up the menu that is shown in Figure 98 on page 136.
Settings	Press this button if you want to change the parameters for any item in the configuration list. This will bring up the menu that is shown in Figure 99 on page 136.
Remove	Press this button if you want to remove an item from the configuration list. You can only remove one item at a time. **Note:** You can only remove an adapter if you have previously removed all protocols that have been associated with that adapter.

Table 17 (Page 2 of 2). Adapter and Protocol Services Installation	
Configuration Item	**Configuration Data**
Change number	Press this button if you need to change the logical sequence in which a protocol driver will address adapters if this protocol has been associated with more than one adapter. Application programs will use these numbers when they issue calls to the network interface(s).

If the LAN adapter in your system is not supplied with OS/2 Warp Server, but you have an NDIS compliant OS/2 device driver for that adapter, click on the **Add adapter** button. The following menu will be shown:

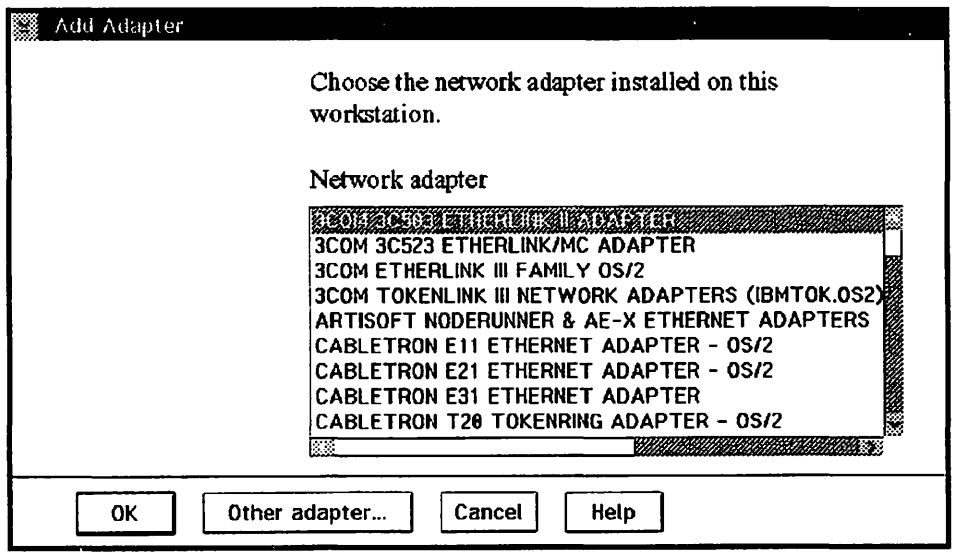

Add Adapter
Choose the network adapter installed on this workstation.
Network adapter
3COM 3C523 ETHERLINK/MC ADAPTER
3COM ETHERLINK III FAMILY OS/2
3COM TOKENLINK III NETWORK ADAPTERS (IBMTOK.OS2)
ARTISOFT NODERUNNER & AE-X ETHERNET ADAPTERS
CABLETRON E11 ETHERNET ADAPTER - OS/2
CABLETRON E21 ETHERNET ADAPTER - OS/2
CABLETRON E31 ETHERNET ADAPTER
CABLETRON T20 TOKENRING ADAPTER - OS/2
OK
Other adapter...
Cancel
Help

Figure 97. Add Adapter Driver to Adapter and Protocol Services

To add a supplied adapter to your configuration, select the appropriate driver from the list, then press **OK**. To add a new adapter driver, select **Other adapter...**, then specify the source drive from where the new driver will be copied to your system.

If you want to use a protocol that is not supplied with OS/2 Warp Server, but you have an NDIS compliant OS/2 device driver for that protocol, click on the **Add protocol** button. The following menu will be shown:

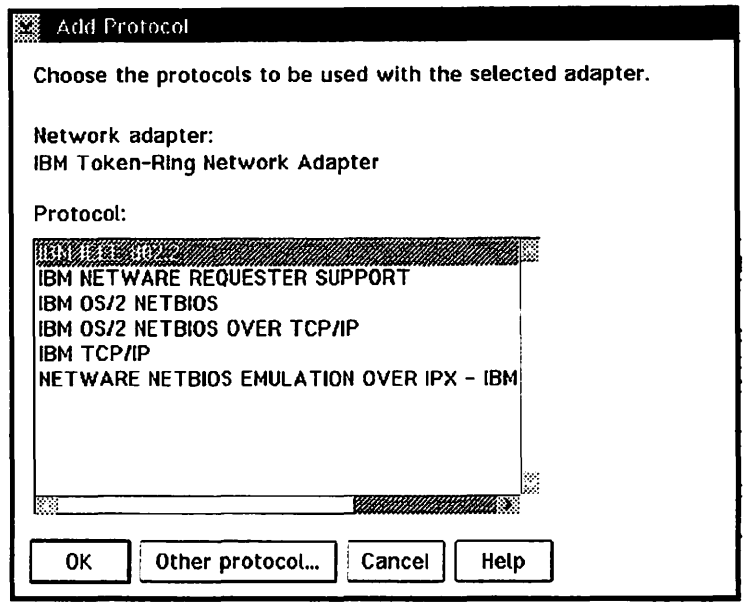


Figure 98. Add Protocol Driver to Adapter and Protocol Services

To add a supplied protocol to your configuration, select the appropriate driver from the list, then press **OK**. To add a new protocol driver, select **Other protocol...**, then specify the source drive from where the new driver will be copied to your system.

Adding an adapter or protocol may affect the configuration of other OS/2 Warp Server components, so you may want to check the items on the configuration tree again. For instance, adding the NetBIOS over TCP/IP protocol will result in another LAN adapter which can be selected for File and Print Sharing Services.

If you want to view or change the configuration of any adapter or protocol driver, select the appropriate item on the list, then click on the **Settings** button. The following menu will be shown:

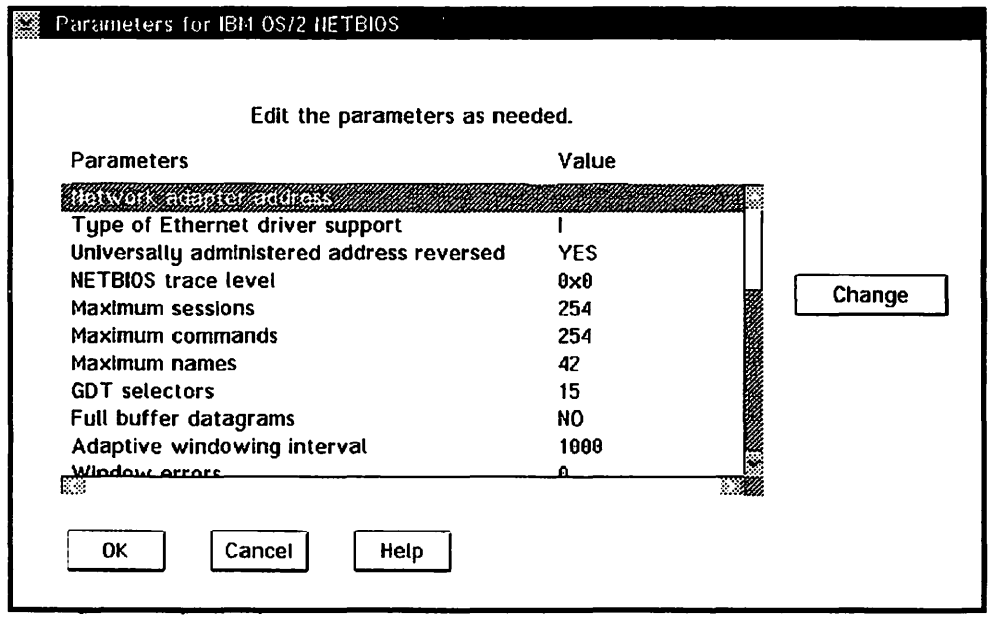


Figure 99. Change Settings in Initial Adapter and Protocol Services Configuration

Note: In this menu, you can only change one item at a time. This is different from the configuration menu that you can use after OS/2 Warp Server has been completely installed. See 4.3, "Additional Configuration for Adapter and Protocol Services" on page 142 for more information on this topic.

Calculating Memory Requirements for Adapter and Protocol Services

Adapter and Protocol Services need to allocate a certain amount of system memory for establishing the protocol stacks that you have selected to use. This section will inform you about how to calculate memory requirements for different protocol stacks.

Some of the following tables and formulas are used as a base for the File and Print Sharing Services Tuning Assistant program which is described in 2.5, "OS/2 Warp Server Tuning Assistant" on page 15.

NetBEUI RAM Usage

The following table summarizes the memory usage of the NetBEUI protocol driver (NETBEUI.OS2). When calculating the total memory requirements, multiply the number of each parameter as specified in the PROTOCOL.INI file by the number of bytes per item as shown in the table below.

Note: All but the requirements for Sessions and Remote Name Cache must fit within a 64KB address space (65535 bytes). The requirements for Sessions and Remote Name Cache will be satisfied from system memory outside that 64KB area.

Table 18. Memory Calculations for NetBEUI

Data area item	Related configuration parameter	RAM usage in bytes
Overhead for device driver memory allocation and communication area		7144
Each NetBIOS session	SESSIONS	700
Each NetBIOS command	NCBS	64
Each NetBIOS name in the local names table	NAMES	76
Each data descriptor to allocate for GDT selectors	SELECTORS	10
Each NetBIOS name in the remote name table (cache)	NAMECACHE	60
Each I-frame packet descriptor	PACKETS	108
Each UI-frame packet descriptor	DATAGRAMPACKETS	124
Each loopback packet descriptor	LOOPPACKETS	148

The following example shows how to calculate RAM usage for NETBEUI parameters, assuming the defaults are being used as specified in the \IBMCOM\PROTOCOL\NETBEUI.NIF file:

```
Parameter              Count      RAM Usage   Parameter Total

Overhead                 1    *    7144    =     7144
Commands               225    *      64    =    14400
```

```
Names                    21    *     76    =    1596
Selectors                15    *     10    =     150
Packets                 350    *    108    =   37800
Datagrampackets          10    *    124    =    1240
Loop Packets              8    *    148    =    1184
-------------------------------------------------------------
check for 64KB limit:                              63514 OK

Sessions                130    *    700    =   91000
Remote Name Cache      1000    *     60    =   60000
=============================================================
Total RAM usage for NETBEUI parameters:           214514
```

TCPBEUI RAM Usage

The following table summarizes the memory usage of the TCPBEUI protocol driver (TCPBEUI.OS2). When calculating the total memory requirements, multiply the number of each parameter as specified in the PROTOCOL.INI file by the number of bytes per item as shown in the table below.

Note: All but the requirements for Sessions and Namecache must fit within a 64KB address space (65535 bytes). The requirements for Sessions and Namecache will be satisfied from system memory outside that 64KB area.

Table 19. Memory Calculations for TCPBEUI

Data area item	Related configuration parameter	RAM usage in bytes
Overhead for device driver memory allocation and communication area		8260
Each NetBIOS session	SESSIONS	382
Each NetBIOS command	NCBS	60
Each NetBIOS name in the local names table	NAMES	91
Each data descriptor to allocate for GDT selectors	SELECTORS	10
Each NetBIOS name in the remote name table (cache)	NAMECACHE	40
Each TCP packet descriptor	PACKETS	114
Each UDP packet descriptor	DATAGRAMPACKETS	1142

The following example shows how to calculate RAM usage for TCPBEUI parameters, assuming the defaults are being used as specified in the \IBMCOM\PROTOCOL\TCPBEUI.NIF file:

```
Parameter              Count      RAM Usage    Parameter Total

Overhead                 1    *    8260    =     8260
Commands               225    *      60    =    13500
Names                   21    *      91    =     1911
Selectors               15    *      10    =      150
Packets                 50    *     114    =     5700
Datagrampackets         20    *    1142    =    22840
-------------------------------------------------------------
check for 64KB limit:                              52361 OK

Sessions               130    *     382    =    49660
Remote Name Cache     1000    *      40    =    40000
```

```
============================================================
Total RAM usage for TCPBEUI parameters:        142021
```

NetBIOS API RAM Usage

The following table summarizes the memory usage of the NetBIOS API driver (NETBIOS.OS2). When calculating the total memory requirements, multiply the number of each parameter as specified in the PROTOCOL.INI file by the number of bytes per item as shown in the table below.

Note: All the requirements for this driver must fit within a 64KB address space (65535 bytes).

Table 20. Memory Calculations for NetBIOS

Data area item	Related configuration parameter	RAM usage in bytes
Overhead for device driver memory allocation and communication area		11310
Commands	Add all NCBS that are specified for all logical adapters which are bound to use the NetBIOS API, then subtract all NCBS that are reserved for the OS/2 LAN Server/Requester redirector (NETWKSTA.SYS) as specified in the \IBMLAN\IBMLAN.INI file, then calculate.	95 * (# of NCBS - # of NCBS used by redirector)
Commands	Add all NCBS that are specified for all logical adapters which are bound to use the NetBIOS API, then subtract all NCBS that are reserved for the OS/2 LAN redirector (NETWKSTA.SYS), as specified in the \IBMLAN\IBMLAN.INI file, then calculate.	15 * (# of NCBS - # of NCBS used by redirector - 15) or 0, if less than 15 NCBS
Adapters	Add all adapters that are bound to the NetBIOS API, as specified in the \IBMCOM\PROTOCOL.INI file, then subtract all adapters that are being used by the OS/2 LAN redirector (NETWKSTA.SYS), as specified in the NETx statement(s) in the \IBMLAN\IBMLAN.INI file, then calculate.	990 * (# of adapters - # of adapters used by redirector)

The following example shows how to calculate RAM usage for the NetBIOS API when using the parameters from the two previous examples, and assuming that:

1. Three adapters are using the NetBIOS API, which can be seen in the following example of a PROTOCOL.INI file:

```
[PROT_MAN]
   DRIVERNAME = PROTMAN$

[NETBIOS]
   DriverName = netbios$
   ADAPTER0 = netbeui$,0
   ADAPTER1 = tcpbeui$,1
   ADAPTER2 = netbeui$,2

[netbeui_nif]
   DriverName = netbeui$
   Bindings = IBMTOKC_nif,,MACETH_nif

[tcpbeui_nif]
   DriverName = tcpbeui$
   Bindings = ,IBMTOKC_nif

[IBMTOK_nif]
   DriverName = IBMTOK$

[MACETH_nif]
   DriverName = MACETH$
```

2. Two adapters are used by the OS/2 LAN redirector, which can be seen in the following example of an IBMLAN.INI file:

```
[networks]
  net1 = netbeui$,0,LM10,34,70,14
  net2 = tcpbeui$,1,LM10,34,70,14
```

Resulting NetBIOS RAM calculation:

```
Parameter               Count     RAM Usage   Parameter Total

Overhead                  1    *   11310    =   11310
# NCBS                   675
# NCBS for redirector  - 140
                        -------
remaining Commands       535    *      95    =   50825
remaining Commands -15   520    *      15    =    7800
# Adapters for API         3
# Adapters for redirector  2
Adapters                  1    *     990    =     990
-------------------------------------------------------------
check for 64KB limit:                                70925 BAD

=============================================================
Total RAM usage for NetBIOS parameters:              70925
```

The NetBIOS API will then not be available to applications that rely on the NB30 NetBIOS interface, such as Systems Management Services and Software Backup and Recovery Services. Applications that can use the LM10 NetBIOS interface, such as File and Print Sharing Services, will not be affected.

To overcome this NetBIOS limit:

1. Increase the number of NCBS that the OS/2 LAN redirector can use to a value of at least 95 each (or a total of 190), or
2. Decrease the number of NCBS per instance of NetBIOS to a value of at most 208 each (or a total of 625).

Note: The LAN Distance logical adapter must be included in the above calculation!

IEEE 802.2 RAM Usage

The following table summarizes the memory usage of the IEEE 802.2 protocol driver (LANDD.OS2). When calculating the total memory requirements, multiply the number of each parameter as specified in the PROTOCOL.INI file by the number of bytes per item as shown in the table below.

Note: All but the requirements for Link Stations (LS) and Timer Control Blocks (TCBs) must fit within a 64KB address space (65535 bytes). The requirements for LS and TCBs will be satisfied from system memory outside that 64KB area.

Table 21. Memory Calculations for IEEE 802.2

Data area item	Related configuration parameter	RAM usage in bytes
Overhead for device driver memory allocation and communication area		5460
Each link stations	LINKS	290
Each service access point (SAP)	MAX_SAPS	120
Each group SAP	MAX_G_SAPS	30
Each application using this interface concurrently	USERS	90
Each I-frame command control block (CCB)	IPACKETS	110
Each UI-, TEST-, XID-, and DIR-frame command control block (CCB)	UIPACKETS	140
Each timer control block (TCB)	TCBS	30

The following example shows how to calculate RAM usage for IEEE 802.2 parameters, assuming the defaults are being used as specified in the \IBMCOM\PROTOCOL\LANDD.NIF file:

```
Parameter                Count      RAM Usage    Parameter Total

Overhead                     1    *     5460    =     5460
Service Access Points        3    *      120    =      360
Group SAPs                   0    *       30    =        0
Users                        3    *       90    =      270
I-frames                   250    *      110    =    27500
UI-frames                  100    *      140    =    14000
-------------------------------------------------------------
check for 64KB limit:                                47590 OK

Link Stations                8    *      290    =     2320
Timer Control Blocks        64    *       30    =     1920
=============================================================
Total RAM usage for IEEE 802.2 parameters            51830
```

4.3 Additional Configuration for Adapter and Protocol Services

If you want to make changes to the configuration of Adapter and Protocol Services after OS/2 Warp Server has been installed, you can easily do so by using the Adapter and Protocol Services configuration program. To start this program, either, click on the **Adapter and Protocol Services** icon in the System Setup folder, or type the following command at an OS/2 command prompt:

```
MPTS
```

Then select **Configure** so it will bring up the panel shown in Figure 100.

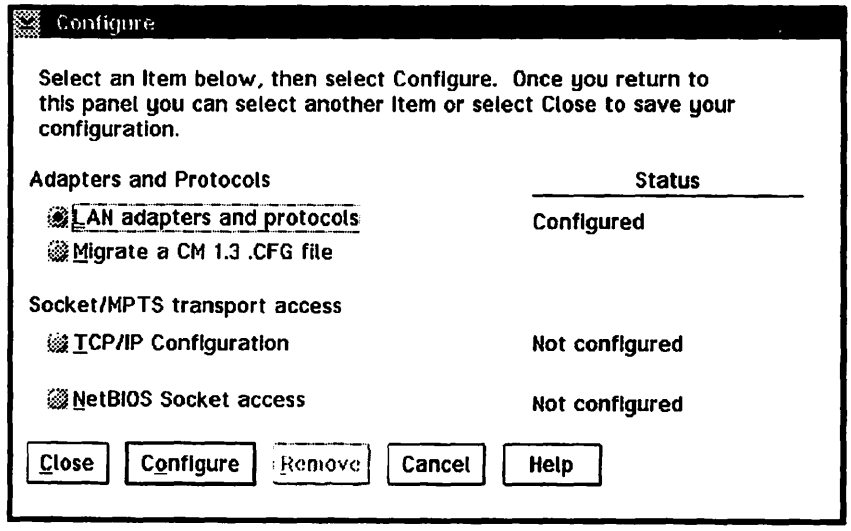


Figure 100. Adapter and Protocol Services - Configure Options

Select LAN adapters and protocols and choose Configure to bring up the LAPS Configuration window. Use this configuration panel to select the LAN adapter(s) installed on the workstation and the protocols associated with them. Figure 101 on page 143 shows an example of what an Adapter and Protocol Services configuration might look like:

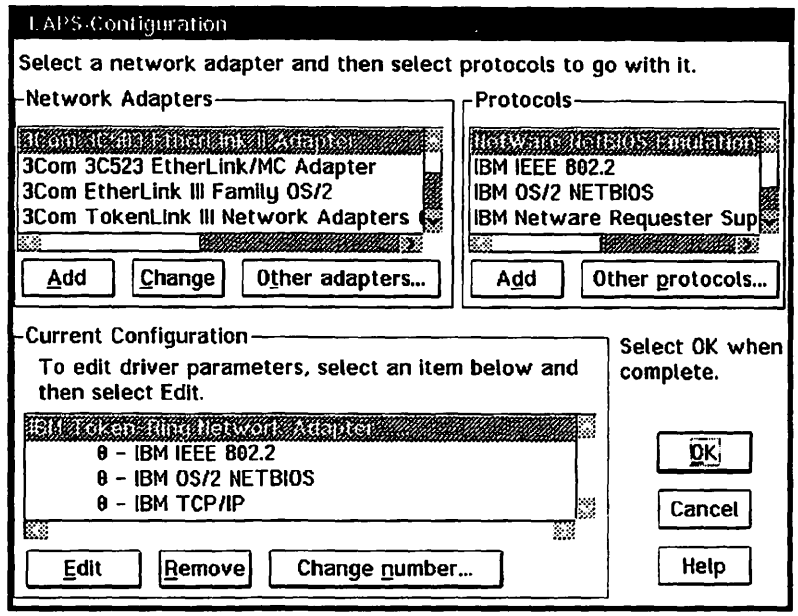


Figure 101. LAPS Configuration

The following table summarizes the use of this configuration menu:

Table 22. Adapter and Protocol Services Configuration	
Configuration Item	**Configuration Data**
Network Adapters window	
Add	Press this button if you want to add an adapter to your configuration.
Change	Press here if you want to change a network adapter for the current configuration.
Other adapters ...	Press this button if you want to add a new adapter driver which is not supplied with Adapter and Protocol Services.
Protocols window	
Add	Press this button if you want to add an adapter to your configuration.
Other protocols ...	Press this button if you want to add a new adapter driver which is not supplied with Adapter and Protocol Services.
Current Configuration window	
Edit	Press here if you want to change the parameters for any item in the configuration list. This will bring up a menu where you can make changes to multiple parameters and then apply all changes at once.
Remove	Press here if you want to remove an item from the configuration list. You can only remove one item at a time. **Note:** You can only remove an adapter if you have previously removed all protocols that have been associated with that adapter.
Change number ...	Press this button if you need to change the logical sequence in which a protocol driver will address adapters if this protocol has been associated with more than one adapter. Application programs will use these numbers when they issue calls to the network interface(s).

If you have finished the configuration, press **OK** to save the changes. Press **Close** on the following panel, then press **Exit**. Select to update the CONFIG.SYS file on the OS/2 boot drive so that the configuration changes can be properly applied. You will need to reboot before the changes will become effective.

Configuring Socket/MPTS

Socket/MPTS is configured from the Configure panel when loading MPTS (see Figure 100 on page 142). Use this panel to select the protocols that you intend to use for Socket access. These selections notify Socket/MPTS to initialize the protocol services required. The selectable protocols are:

1. TCP/IP Socket access
2. NetBIOS Socket access

To select TCP/IP Socket access, you must have the TCP/IP protocol configured (using the LAN adapters and protocols configuration option). To select NetBIOS Socket access, you must have the NetBIOS protocol configured (using the LAN adapters and protocols configuration option). You must select at least one protocol for your Socket/MPTS environment. However, you can select more than one protocol.

Note: When you have installed TCP/IP Services, during the initial installation of your OS/2 Warp Server system or at any later time, you must use the TCP/IP Configuration notebook to configure TCP/IP parameters. In this case, the status text of the TCP/IP Configuration in the Configure menu (shown in Figure 100 on page 142) will inform you about this, and the Configure button will be grayed out.

Please see 5.3, "Additional Configuration for TCP/IP Services" on page 173 for more information on how to use the TCP/IP Configuration notebook.

Configuring TCP/IP Socket Access

Select TCP/IP Socket access, then click on **Configure**. The following menu will be shown:

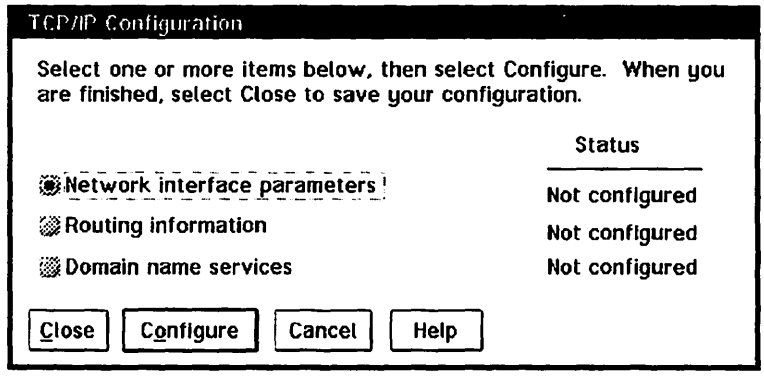


Figure 102. TCP/IP Socket Access Configuration

On this page, you can select what parts of the TCP/IP Socket access you want to configure.

Select Network Interfaces, then click on **Configure**. The following menu will be shown:

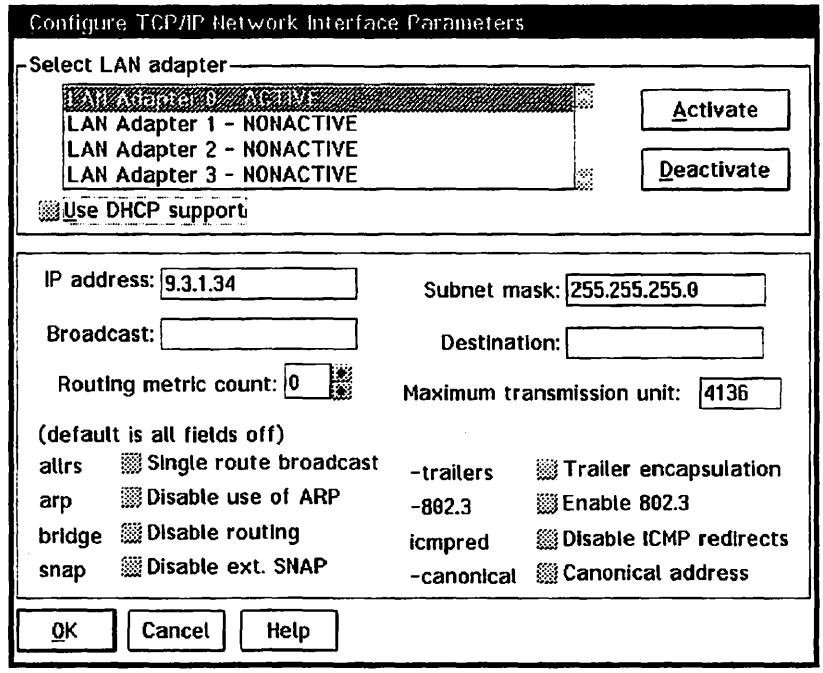


Figure 103. TCP/IP Network Interface Configuration

On this page, you can configure the TCP/IP network interfaces of your OS/2 Warp Server system. The following table summarizes the configuration parameters of this page and describes their purposes.

Table 23 (Page 1 of 2). TCP/IP Network Interface Configuration

Configuration Item	Configuration Data
Select LAN adapter	Select a LAN adapter, then click on **Activate** to make it available for TCP/IP Socket access.
Use DHCP support	Check, if you want the DHCP client to automatically configure this interface with parameters obtained from a DHCP server, if one exists on the network.
IP address	The IP address of this interface to the IP network
Subnet mask	This is the value obtained from your network coordinator to define the network range of your IP address.
Broadcast	The broadcast address for your IP network, derived from the combination of your IP address and subnet mask. This will be calculated automatically by TCP/IP.
Destination address	The base address of your IP network, derived from the combination of your IP address and subnet mask. This will be calculated automatically by TCP/IP.
Metric count	The number of hops that can be used to access another IP address.
Maximum transmission unit	Specify the maximum IP packet size for that interface. The default is 1500 bytes.

Table 23 (Page 2 of 2). TCP/IP Network Interface Configuration	
Configuration Item	**Configuration Data**
Single route broadcast	Use this field to set the token ring broadcast indicator. All-Routes broadcast allrs is the default.
Disable use of ARP	Use this field to enable the use of the Address Resolution Protocol (ARP) for mapping between IP addresses and LAN adapter addresses. Default is enabled.
Disable routing	Use this field to enable source routing information in token-ring packets.
Disable extended SNAP	Use this field to send TCP/IP packets with headers that have the extended SNAP header format.
Trailer encapsulation	Use this field to request the use of a trailer link level encapsulation when sending messages.
Enable 802.3	Use this field to disable Ethernet 802.3 and enable Ethernet DIX2.
Disable ICPM redirects	Use this field to allow or deny TCP/IP to add routes obtained by ICMP redirects.
Canonical address	Use this field to indicate that MAC addresses in the Address Resolution Protocol (ARP) packet on this token-ring network are in the canonical IEEE 802.5 form.

Click on **OK** to finish this configuration.

If you want to use DHCP to automatically configure the TCP/IP parameters for your OS/2 Warp Server system, click on **DHCP**. The Network Interface Configuration menu will now look as shown in the figure below:

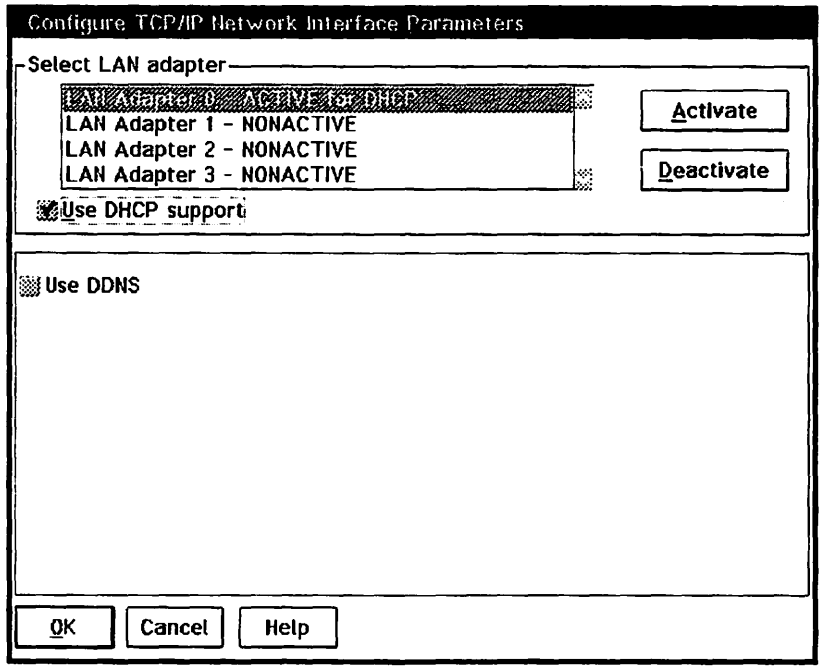


Figure 104. TCP/IP Network Interface Configuration Using DHCP

On this page, you can only select whether or not you want to use DDNS in addition to DHCP. All other parameters will be set according to the information that the DHCP client will retrieve from a DHCP server when you restart the system.

Click on **OK** to finish this configuration.

The remaining configuration options need not be selected if you chose to use DHCP with this system but you can configure them if you need to.

Select Routing Information, then click on **Configure**. This will bring up a menu similar to Figure 127 on page 178. See "Configure Routers" on page 178 for more information on how to configure TCP/IP routing information.

Click on **OK** to finish this configuration.

Select **Nameserver**, then click on **Configure**. This will bring up a menu similar to Figure 129 on page 180. See "Configure Hostnames and Nameservers" on page 179 for more information on how to configure TCP/IP nameserver information.

Click on **OK** to finish this configuration.

When you finished the TCP/IP Socket access configuration, click on **Close** to return to the Configuration menu.

Configuring NetBIOS Socket Access

Select NetBIOS Socket access, then click on **Configure**. The following menu will be shown:

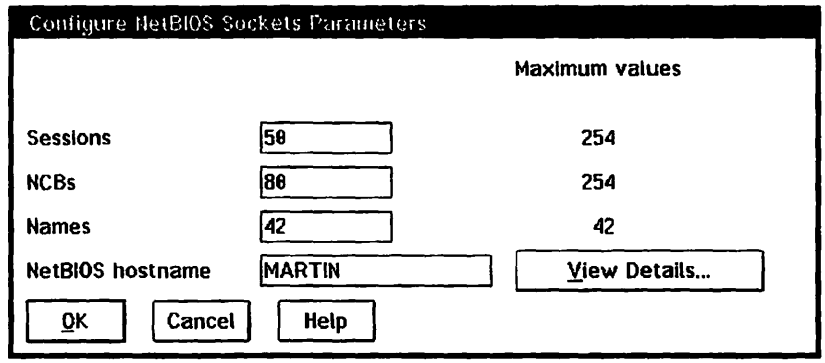


Figure 105. Sockets Access Configuration

On this page, you can configure the NetBIOS interfaces of your OS/2 Warp Server system for Socket access. The following table summarizes the configuration parameters of this page and describes their purposes.

Table 24. NetBIOS Interface Configuration for Socket Access	
Configuration Item	**Configuration Data**
Sessions	Specify the number of NetBIOS sessions that you want to reserve for Sockets applications. The number of sessions specified here will be taken from the total amount of sessions specified in the NETBEUI section of the PROTOCOL.INI file. This means that the amount of sessions available to other NetBIOS applications, such as File and Print Sharing Services, will be reduced by the number specified here.
NCBs	Specify the number of NetBIOS commands (NCBs) that you want to reserve for Sockets applications. The number of NCBs specified here will be taken from the total amount of NCBs specified in the NETBEUI section of the PROTOCOL.INI file. This means that the number of NCBs available to other NetBIOS applications, such as File and Print Sharing Services, will be reduced by the number specified here.
Names	Specify the number of NetBIOS names that you want to reserve for Sockets applications. The number of names specified here will be taken from the total amount of names specified in the NETBEUI section of the PROTOCOL.INI file. This means that the amount of names available to other NetBIOS applications, such as File and Print Sharing Services, will be reduced by the number specified here.
NetBIOS hostname	Enter the hostname that your NetBIOS Sockets applications will be using.
View Details...	Click here to see more available hostnames. When the NetBIOS protocol is configured to more than one adapter, Socket/MPTS will use the hostname that you have specified for the first interface, and it will add to that name unique identifiers (consecutive numbers) and use that as hostnames for the other interfaces.

When you finished the TCP/IP Socket access configuration, click on **Close** to return to the Configuration menu.

You can use the NETSTAT program to see if the NetBIOS Sockets interface is initialized, and what applications are currently using it.

Removing Socket/MPTS Configuration

When you want to remove a Socket/MPTS configuration from your OS/2 Warp Server system, you can do it from the Configure panel when loading MPTS (see Figure 100 on page 142). Select the appropriate Socket access protocol to be removed (TCP/IP or NetBIOS), then click on **Remove**. If you want to remove both protocols, you can do so by removing one after the other.

Note: Removing a Socket access protocol will not remove the protocol driver from the LAN adapter and protocol configuration. It will only update the \MPTN\BIN\MPTCONFG.INI file and remove device drivers from the CONFIG.SYS file.

New Configuration Parameters for NetBEUI Protocol Driver

The NETBEUI section of the PROTOCOL.INI file has two configurable parameters that are not listed before in the formal documentation, SIDEBAND and BALANCE. These parameters should not be changed from their default values. When not present in the PROTOCOL.INI file, these two parameters are set to the correct values automatically. The default values (when not present in PROTOCOL.INI) are as follows:

```
SIDEBAND = 1
BALANCE  = 2
```

Setting `SIDEBAND to 1` enables a performance enhancement used by File and Print Sharing Services for sending small frames. Setting `SIDEBAND to 0` disables this performance enhancement.

BALANCE is used to control how NetBEUI chooses which adapters are used when an NCB.LISTEN command is issued on a machine with multiple network adapters. If two network adapters on the same machine are on the same network segment (bridged segment) then setting BALANCE to 0 disables load balancing, setting BALANCE to 1 puts it into load balancing mode and setting BALANCE to 2 lets NetBEUI decide the appropriate load balancing mode.

Configuring Adapter and Protocol Services for more than Four LAN Adapters

Adapter and Protocol Services itself is not limited to four adapters as is the NB30 NetBIOS API, as discussed below. Adapter and Protocol Services support includes LAN adapters as well as other NDIS communication adapter drivers, such as asynchronous and parallel port support, WAN and ISDN. The number of adapter drivers that can actually be used concurrently differs between the NDIS protocol drivers. The TCP/IP, IEEE 802.2 and NetWare Requester Support protocol drivers can support up to 64 adapters. The NetBIOS protocol drivers (IBM NETBEUI, IBM NetBIOS over TCP/IP, NetWare NetBIOS Emulation) will only support four adapters, which is the limit of the NB30 NetBIOS API.

Since all NetBIOS drivers that are supplied with OS/2 Warp Server also support the LM10 NetBIOS API, there is no restriction to four adapters when this interface is used by applications. This will increase the number of clients that can be simultaneously connected to OS/2 Warp Server over NetBIOS. It will also help the session load balancing performed by File and Print Sharing Services.

In the following example, we used four DUAL Auto LANStreamer adapter cards that provide two separate token-ring ports each. This gives us a total of eight LAN adapters as seen by NDIS. Figure 106 on page 150 shows how these adapters can be interfaced by NetBIOS applications. NB30 applications will only be able to interface with four adapters, whereas LM10 applications, such as File and Print Sharing Services, will be able to interface with all eight adapters which are bound to the NetBEUI protocol driver.

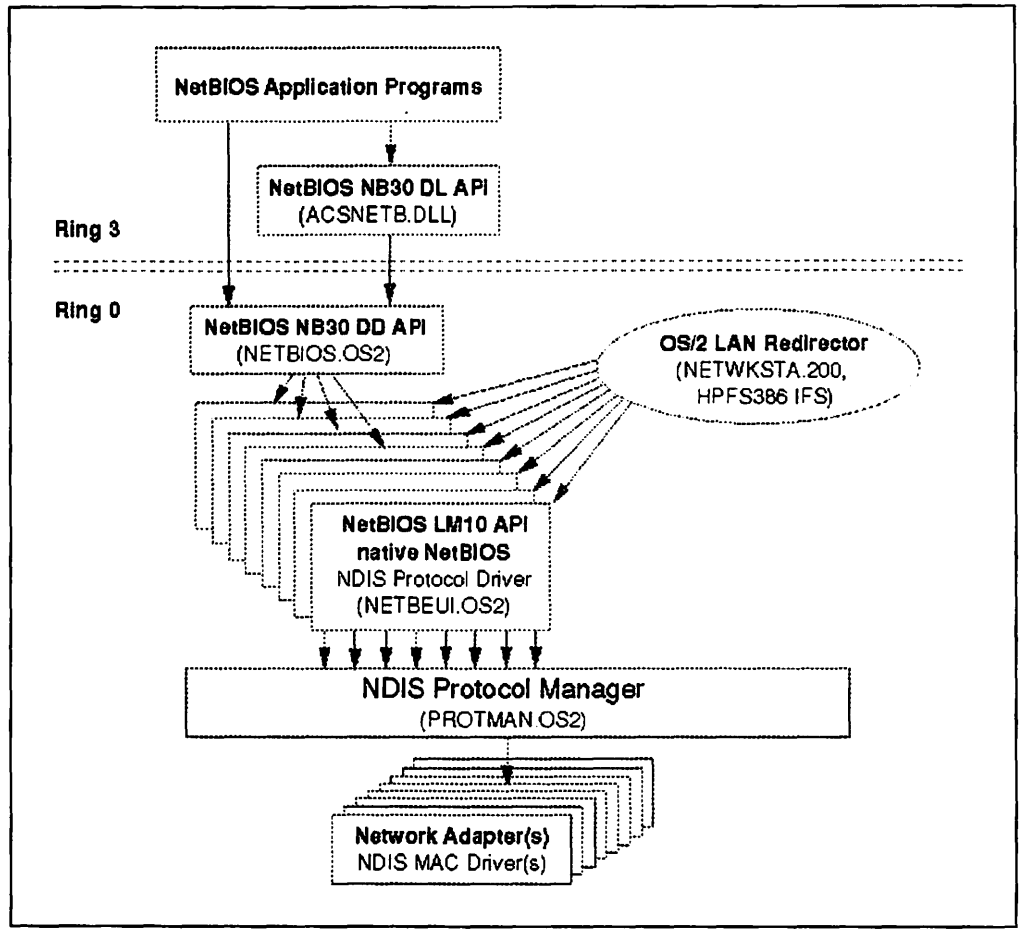


Figure 106. NetBIOS Configuration for Eight Adapters

The following lines are extracted from the CONFIG.SYS file to reflect what drivers must be loaded in order to support the configuration as shown above:

```
...
DEVICE=C:\IBMCOM\MACS\DUALSTRM.OS2 /S:3
DEVICE=C:\IBMCOM\MACS\DUALSTRM.OS2 /S:4
DEVICE=C:\IBMCOM\MACS\DUALSTRM.OS2 /S:6
DEVICE=C:\IBMCOM\MACS\DUALSTRM.OS2 /S:7
DEVICE=C:\IBMCOM\LANMSGDD.OS2 /I:C:\IBMCOM
DEVICE=C:\IBMCOM\PROTMAN.OS2 /I:C:\IBMCOM
...
```

Notes:

1. You have to add the lines for the DUALSTRM.OS2 device driver manually.
2. Make sure you add those lines before the PROTMAN.OS2 device driver statement, as shown in the example above.
3. Include the */S* parameter on every statement to specify the slot that the Dual LANStreamer adapter is plugged into.

The following lines are extracted from the PROTOCOL.INI file to reflect what drivers must be loaded to support the configuration as shown above:

```
[PROT_MAN]
   DRIVERNAME = PROTMAN$
[IBMLXCFG]
```

```
   netbeui_nif = netbeui.nif
   IBMMPC_nif = IBMMPC.NIF
   IBMMPC_nif2 = ibmmpc.nif
   IBMMPC_nif3 = ibmmpc.nif
   IBMMPC_nif4 = ibmmpc.nif
   IBMMPC_nif5 = ibmmpc.nif
   IBMMPC_nif6 = ibmmpc.nif
   IBMMPC_nif7 = ibmmpc.nif
   IBMMPC_nif8 = ibmmpc.nif

[NETBIOS]

   DriverName = netbios$
   ADAPTER0 = netbeui$,0
   ADAPTER1 = netbeui$,1
   ADAPTER2 = netbeui$,2
   ADAPTER3 = netbeui$,3
;
; only four adapters may be initialized here - that's the NB30 interface
;

[netbeui_nif]

   DriverName = netbeui$
   Bindings = IBMMPC_nif,IBMMPC_nif2,IBMMPC_nif3,IBMMPC_nif4,
              IBMMPC_nif5,IBMMPC_nif6,IBMMPC_nif7,IBMMPC_nif8
;
; the Bindings statement must go on a single line
;
   ETHERAND_TYPE = "I"
   USEADDRREV = "YES"
   OS2TRACEMASK = 0x0
   SESSIONS = 254
   NCBS = 254
   NAMES = 42
   SELECTORS = 15
   USEMAXDATAGRAM = "NO"
   ADAPTRATE = 1000
   WINDOWERRORS = 0
   MAXDATARCV = 4352
   TI = 30000
   T1 = 1000
   T2 = 200
   MAXIN = 1
   MAXOUT = 1
   NETBIOSTIMEOUT = 2000
   NETBIOSRETRIES = 3
   NAMECACHE = 1000
   RNDOPTION = 1
   PIGGYBACKACKS = 1
   DATAGRAMPACKETS = 10
   PACKETS = 330
   LOOPPACKETS = 8
   PIPELINE = 5
   MAXTRANSMITS = 6
   MINTRANSMITS = 2
   DLCRETRIES = 10
   FCPRIORITY = 5
   NETFLAGS = 0x1000

[IBMMPC_nif]

   DriverName = IBMMPC$
   MaxTransmits = 31
   MaxTxFrameSize = 18000
   MinRcvBuffs = 20
   SizWorkBuf = 2048
   MulticastNum = 16
   EnableTxEofInt = "YES"
   Enet20UTP = "NO"
   EnableHiPriTx = "NO"
   HiPriTxAccess = 5
   HiPriTxThresh = 4
   LLCOnly = "NO"

[IBMMPC_nif2]

   DriverName = IBMMPC$
   MaxTransmits = 31
   MaxTxFrameSize = 18000
   MinRcvBuffs = 20
   SizWorkBuf = 2048
```

```
   MulticastNum = 16
   EnableTxEofInt = "YES"
   Enet20UTP = "NO"
   EnableHiPriTx = "NO"
   HiPriTxAccess = 5
   HiPriTxThresh = 4
   LLCOnly = "NO"

[IBMMPC_nif3]

   DriverName = IBMMPC$
   MaxTransmits = 31
   MaxTxFrameSize = 18000
   MinRcvBuffs = 20
   SizWorkBuf = 2048
   MulticastNum = 16
   EnableTxEofInt = "YES"
   Enet20UTP = "NO"
   EnableHiPriTx = "NO"
   HiPriTxAccess = 5
   HiPriTxThresh = 4
   LLCOnly = "NO"

[IBMMPC_nif4]

   DriverName = IBMMPC$
   MaxTransmits = 31
   MaxTxFrameSize = 18000
   MinRcvBuffs = 20
   SizWorkBuf = 2048
   MulticastNum = 16
   EnableTxEofInt = "YES"
   Enet20UTP = "NO"
   EnableHiPriTx = "NO"
   HiPriTxAccess = 5
   HiPriTxThresh = 4
   LLCOnly = "NO"

[IBMMPC_nif5]

   DriverName = IBMMPC$
   MaxTransmits = 31
   MaxTxFrameSize = 18000
   MinRcvBuffs = 20
   SizWorkBuf = 2048
   MulticastNum = 16
   EnableTxEofInt = "YES"
   Enet20UTP = "NO"
   EnableHiPriTx = "NO"
   HiPriTxAccess = 5
   HiPriTxThresh = 4
   LLCOnly = "NO"

[IBMMPC_nif6]

   DriverName = IBMMPC$
   MaxTransmits = 31
   MaxTxFrameSize = 18000
   MinRcvBuffs = 20
   SizWorkBuf = 2048
   MulticastNum = 16
   EnableTxEofInt = "YES"
   Enet20UTP = "NO"
   EnableHiPriTx = "NO"
   HiPriTxAccess = 5
   HiPriTxThresh = 4
   LLCOnly = "NO"

[IBMMPC_nif7]

   DriverName = IBMMPC$
   MaxTransmits = 31
   MaxTxFrameSize = 18000
   MinRcvBuffs = 20
   SizWorkBuf = 2048
   MulticastNum = 16
   EnableTxEofInt = "YES"
   Enet20UTP = "NO"
   EnableHiPriTx = "NO"
   HiPriTxAccess = 5
   HiPriTxThresh = 4
   LLCOnly = "NO"
```

```
[IBMMPC_nif8]

   DriverName = IBMMPC$
   MaxTransmits = 31
   MaxTxFrameSize = 18000
   MinRcvBuffs = 20
   SizWorkBuf = 2048
   MulticastNum = 16
   EnableTxEofInt = "YES"
   Enet20UTP = "NO"
   EnableHiPriTx = "NO"
   HiPriTxAccess = 5
   HiPriTxThresh = 4
   LLCOnly = "NO"
```

The following lines are extracted from the LANTRAN.LOG file to reflect what messages will be logged when the Adapter and Protocol Services device drivers are initialized, when a configuration as shown above is being used:

```
LT00073: FFST/2 is installed but is not started.  LANTRAN.LOG is being
IBM OS/2 LANMSGDD [11/03/95] 2.01 is loaded and operational.
IBM OS/2 LAN Protocol Manager
IBM - OS/2 Socket/MPTS Common Transport Semantics
IBM OS/2 NETBEUI 5.00.0
NETBEUI: Using a 32-bit data segment.
Installing NETWKSTA.200 Version 5.0. IBM LAN Redirector (Nov 06, 1995)

IBM OS/2 NETBIOS 4.0
Adapter 0 has 34 NCBs, 153 sessions, and 28 names available to NETBIOS applications.
Adapter 1 has 34 NCBs, 153 sessions, and 28 names available to NETBIOS applications.
Adapter 2 has 34 NCBs, 153 sessions, and 28 names available to NETBIOS applications.
Adapter 3 has 34 NCBs, 153 sessions, and 28 names available to NETBIOS applications.
NETBIOS 4.0 is loaded and operational.
IBM Streamer Family adapter NDIS device driver Version 4.01.00
Initialization proceeding for section IBMMPC_NIF in PROTOCOL.INI
Initialization proceeding for section IBMMPC_NIF2 in PROTOCOL.INI
Initialization proceeding for section IBMMPC_NIF3 in PROTOCOL.INI
Initialization proceeding for section IBMMPC_NIF4 in PROTOCOL.INI
Initialization proceeding for section IBMMPC_NIF5 in PROTOCOL.INI
Initialization proceeding for section IBMMPC_NIF6 in PROTOCOL.INI
Initialization proceeding for section IBMMPC_NIF7 in PROTOCOL.INI
Initialization proceeding for section IBMMPC_NIF8 in PROTOCOL.INI
IBM LANVDD is loaded and operational.
IBM OS/2 LAN Netbind
Slot 3A:  IBM Streamer Family adapter universal address is 08005a6c072c
Slot 3A:  IBM Streamer Family adapter opened for:  Token Ring, 16 Mbps.
Slot 3B:  IBM Streamer Family adapter universal address is 08005a6c072d
Slot 3B:  IBM Streamer Family adapter opened for:  Token Ring, 16 Mbps.
Slot 4A:  IBM Streamer Family adapter universal address is 08005a6c08a8
Slot 4A:  IBM Streamer Family adapter opened for:  Token Ring, 16 Mbps.
Slot 4B:  IBM Streamer Family adapter universal address is 08005a6c08a9
Slot 4B:  IBM Streamer Family adapter opened for:  Token Ring, 16 Mbps.
Slot 6A:  IBM Streamer Family adapter universal address is 08005a6cd11a
Slot 6A:  IBM Streamer Family adapter opened for:  Token Ring, 16 Mbps.
Slot 6B:  IBM Streamer Family adapter universal address is 08005a6cd11b
Slot 6B:  IBM Streamer Family adapter opened for:  Token Ring, 16 Mbps.
Slot 7A:  IBM Streamer Family adapter universal address is 08005a1e4772
Slot 7A:  IBM Streamer Family adapter opened for:  Token Ring, 16 Mbps.
Slot 7B:  IBM Streamer Family adapter universal address is 08005a1e4773
Slot 7B:  IBM Streamer Family adapter opened for:  Token Ring, 16 Mbps.
```

The following lines are extracted from the IBMLAN.INI file to reflect what statements must be configured to support the configuration as shown above:

```
[networks]

  net1 = NETBEUI$,0,LM10,101,220,14
  net2 = NETBEUI$,1,LM10,101,220,14
  net3 = NETBEUI$,2,LM10,101,220,14
  net4 = NETBEUI$,3,LM10,101,220,14
  net5 = NETBEUI$,4,LM10,101,220,14
  net6 = NETBEUI$,5,LM10,101,220,14
  net7 = NETBEUI$,6,LM10,101,220,14
  net8 = NETBEUI$,7,LM10,101,220,14

...

[requester]

...
  wrknets = net1,net2,net3,net4,net5,net6,net7,net8
```

```
...
[server]
...
  srvnets = net1,net2,net3,net4,net5,net6,net7,net8
...
```

4.4 Useful Adapter and Protocol Services Applets

Adapter and Protocol Services provides additional utility programs that can be very helpful in assisting the planning, configuration and problem-determination processes of an OS/2 Warp Server system. These programs are contained in the MPTSAPLT.ZIP file in the \CID\SERVER\IBMLS\IBM500N5\APPLETS directory on the OS/2 Warp Server CD-ROM. To install the programs, unzip that file into any directory on your hard drive that is included in the PATH= statement in CONFIG.SYS.

This section describes some of the applets programs; a complete description is provided in the *MPTS Configuration Guide* online book on the OS/2 Warp Server desktop. You can find it by opening the Information folder, then LAN Services File and Print folder.

NB64K Utility: This program checks a given NetBIOS configuration for the amount of memory that will be used and whether that amount will be within certain limits, as described in "Calculating Memory Requirements for Adapter and Protocol Services" on page 137. Figure 107 shows the NB64K program performing a check on the NETBEUI default parameters:

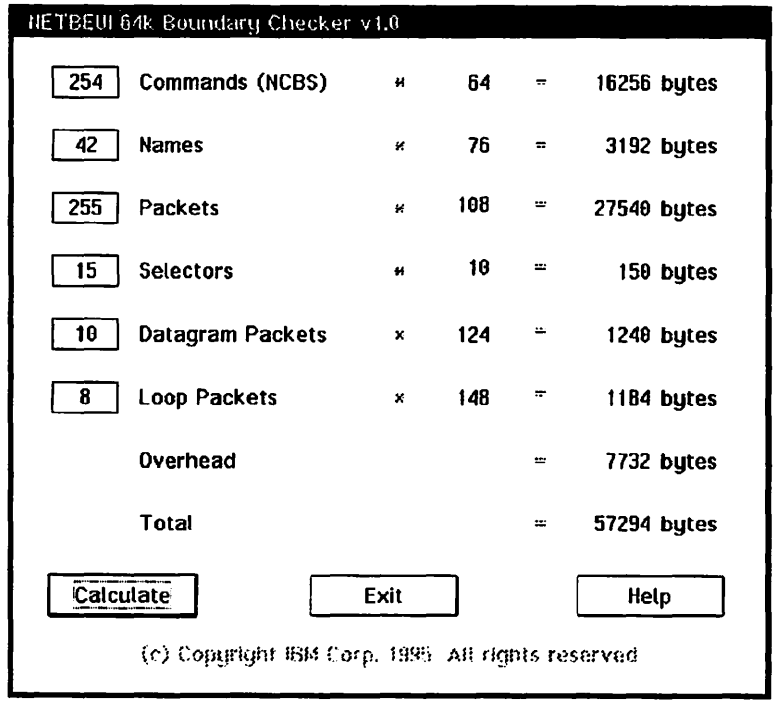

NETBEUI 64k Boundary Checker v1.0
254 Commands (NCBS) * 64 = 16256 bytes
42 Names * 76 = 3192 bytes
255 Packets * 108 = 27540 bytes
15 Selectors * 10 = 150 bytes
10 Datagram Packets * 124 = 1240 bytes
8 Loop Packets * 148 = 1184 bytes
Overhead = 7732 bytes
Total = 57294 bytes
Calculate
Exit
Help
(c) Copyright IBM Corp. 1995 All rights reserved

Figure 107. NB64K Utility

NBJDSTAT Utility: This program can be used to display the status of the NetBIOS protocol on any of the four adapters that can be used with the NB30 interface. A search for specific application names can be performed, such as

DB2/2 and RFC NetBIOS names. The example below shows the output of a possible status of all parameters for one instance of the NetBIOS protocol:

```
NBJDSTAT  V2.00
Copyright IBM 1992-1994

Return Code from NCB.STATUS 0x0

Universal Adapter Address 89EACE5A0000

Software release number.....................4
Reserved field..............................0
Software Number.............................40FF..Netbios 4.0..Token Ring
Reporting period in minutes (since NCB reset)..1440
Number of FRMR frames received..............0
Number of FRMR frames transmitted...........0
Number of I frames received in error........0
Number of aborted transmissions.............0
Number of successfully transmitted packets.....7586
Number of successfully received packets........49894
Number of I frames transmitted in error.....0
Times a buffer was not present..............0
Number of times DLC t1 expired..............0
Number of times DLC ti expired..............732
---Extended status table---
Dir init bring up error......0
Dir open adapter error.......0
Latest network status........0
Latest adapter check.........0
Latest pc detected error.....0
Latest operational cmd error.0
CCB rc.......................0
Line error...................0
Internal error...............0
Burst errors.................0
ARI fci delimiter............0
Abort delimiter..............0
Resvered1....................0
Lost frame...................0
Receive congestion...........0
Frame copy error.............0
Frequency error..............0
Token error..................0
Reserved2....................0
DMA bus error................0
DMA parity error.............0
Local address................00005ACEEA89
Number of Free NCBs.............................217
Configured NCB maximum.........................225
Maximum NCBs...................................225
Local station busy count.......................0
Maximum datagram packet........................512
Number of pending sessions.....................7
Configured session maximum.....................130
Maximum sessions...............................130
Maximum session packet.........................4168
Number of names in table.......................7
Name                                  Name #   Status
MURLI                                  002     04 Unique   Registered name
0x4d55524c492020202020202020202000

MURLI         ♥                        003     04 Unique   Registered name
0x4d55524c492020202020202020202003

ITSCAUS                                004     84 Group    Registered name
0x4954534341555320202020202020200

NQSPM2.MURLI0                          005     04 Unique   Registered name
0x4e5153504d322e4d55524c4930000000

MURLI                                  006     04 Unique   Registered name
0x4d55524c492020202020202020202020

NQ.ACTIVE.SPM2                         007     84 Group    Registered name
0x4e512e4143544956452e53504d320000

A948R2        ♥                        008     04 Unique   Registered name
0x4139343852322020202020202020203
```

The NBJDSTAT program can be used with the following options:

```
NBJDSTAT  V2.00
Copyright IBM 1992-1994

Usage:nbjdstat remote_name options
    remote_name:NETBIOS name to find(length: 16 characters [case sensitive])
       If the name is less than 16 characters, blanks(0x20) are appended.
       * specifies local name.
    options:
       /a  :specifies adapter to use (default:0) - valid:0,1,2,3
       /h  :intrepet value as hex value and append to remote name
            example: SERVER1 /h20
            entire remote name may be specified as hex value
            example: /h4155532020202020202020202020202020
       /m  :to make the name as IBM LS messenger name
       /n  :to append 0x00 to the name up to 16 characters
       /q  :to make the name as IBM LS requester name
       /v  :to make the name as IBM LS server name
       /rxy:to make the name as IBM DB2/2 requester name
            x can be: s(sql name); i(interrupt name)
            y can be: 0(adapter 0); 1(adapter 1)
       /sxy:to make the name as IBM DB2/2 server name
            if x: is c(catcher name))
            y can be: 0(adapter 0); 1(adapter 1)
            if x: is b(callback name)
            y can be: p(primary adapter); s(secondary adapter)
```

NETPING Utility: This program can be used to query NetBIOS names on a network to check if a server system or partner application is actually active. Any of the four adapters that are supported by the NB30 interface can be used with a NETPING command. A search for specific application names can be performed, such as DB2/2 NetBIOS names. The example below shows a search for the name W4602S00:

```
NETPING  V2.00
Copyright IBM 1992-1994

Finding the name "W4602S00        " in the network ...
                 0123456789ABCDEF

Name Type   : UNIQUE
MAC Address : 0800 5a6c 072c
Route       :  e30 <- 011 <- 01b
Target is here -^
You are here -----------------^
```

Figure 108. NETPING Utility

The NETPING program can be used with the following options:

```
NETPING  V2.00
Copyright IBM 1992-1994

Userage:netping name options
    name:NETBIOS name to find(length: 16 characters [case sensitive])
       If the name is less than 16 characters, blanks(0x20)
```

```
   will be used to fill the name up to 16 characters.
options:
   /a  :specifies adapter to use (default:0)
        valid adapter: 0,1,2,3
   /m  :to make the name as IBM LS messenger name
   /n  :to append 0x00 to the name up to 16 characters
   /q  :to make the name as IBM LS requester name
   /v  :to make the name as IBM LS server name
   /rxy:to make the name as IBM DB2/2 requester name
        x can be: s(sql name); i(interrupt name)
        y can be: 0(adapter 0); 1(adapter 1)
   /sxy:to make the name as IBM DB2/2 server name
        if x: is c(catcher name))
        y can be: 0(adapter 0); 1(adapter 1)
        if x: is b(callback name)
        y can be: p(primary adapter); s(secondary adapter)
```

MAPNAME Utility: This program encodes and decodes NetBIOS names to and from names that can be used with the TCP/IP Domain Name System, as specified in RFCs 1001/1002. Please see "Storing NetBIOS Names on the Domain Nameserver" on page 266 on how to effectively use the MAPNAME program.

4.5 NetWare Requester for OS/2

OS/2 Warp Server provides the OS/2 requester program and protocols to access Novell NetWare servers and other systems that are using NetWare protocols in the network. It is, however, the purpose of this section to introduce the network protocols that the NetWare Requester is using, not to describe the NetWare Requester itself or any of its functions.

Whereas Adapter and Protocol Services is an implementation of the NDIS architecture, Novell and Apple have jointly developed their own solution for multiprotocol networked environments - The Open Data-Link Interface (ODI).

Figure 109 on page 158 illustrates ODI in relation to the OSI Model and the four main components of ODI. These are:

- Network Protocol Drivers - (similar to NDIS protocol drivers)
- Link Support Layer (LSL) - (similar in some respects to the NDIS interface)
- Multiple Link Interface Driver (MLID) - (similar to NDIS MAC driver)
- Control File - NET.CFG

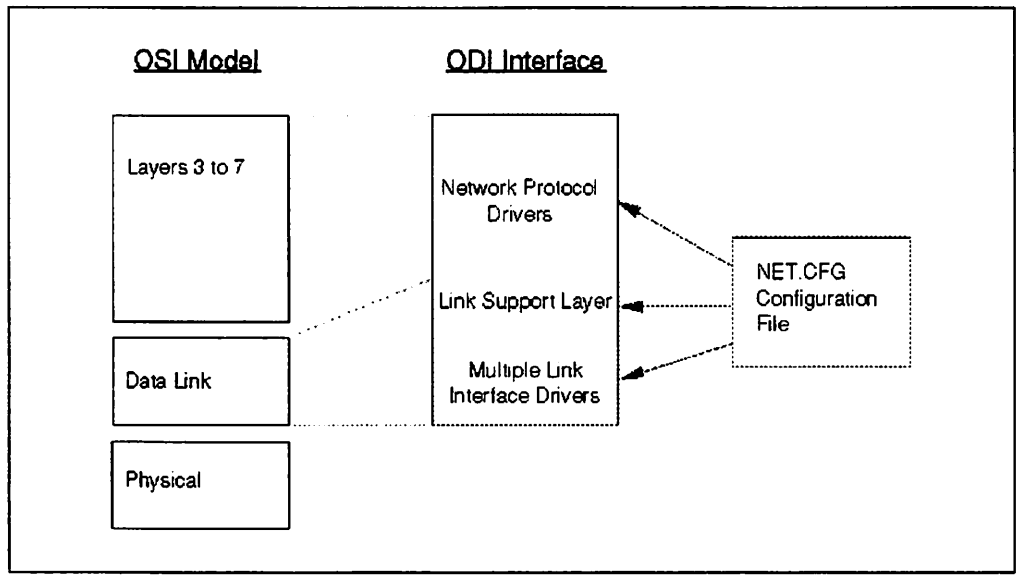


Figure 109. ODI Stack

By default, the NetWare Requester would run on an ODI stack. The normal NetWare protocol driver is IPX, for which there is no NDIS protocol driver available. However, it is not possible to have both an NDIS MAC driver and an ODI MLID loaded simultaneously for the same adapter. So, it is not possible, for example, to run the NetWare Requester on a full ODI stack and File and Print Sharing Services on an NDIS stack at the same time.

To run the NetWare Requester over the NDIS interface, IBM has developed a special driver: ODI2NDI (or ODI to NDIS). This driver may be loaded from the Adapter and Protocol Services configuration panel like any protocol driver. ODI2NDI provides an interface to the ODI stack so that the NetWare protocol drivers are able to use the NDIS interface and to coexist with NDIS protocol drivers. Figure 110 on page 159 shows the protocol stacks in use when the NetWare Requester is coexisting with the IBM LAN requester. Please observe that the ODI2NDI driver, which appears to the NDIS interface as a protocol driver, appears to the ODI stack as an adapter driver (MLID).

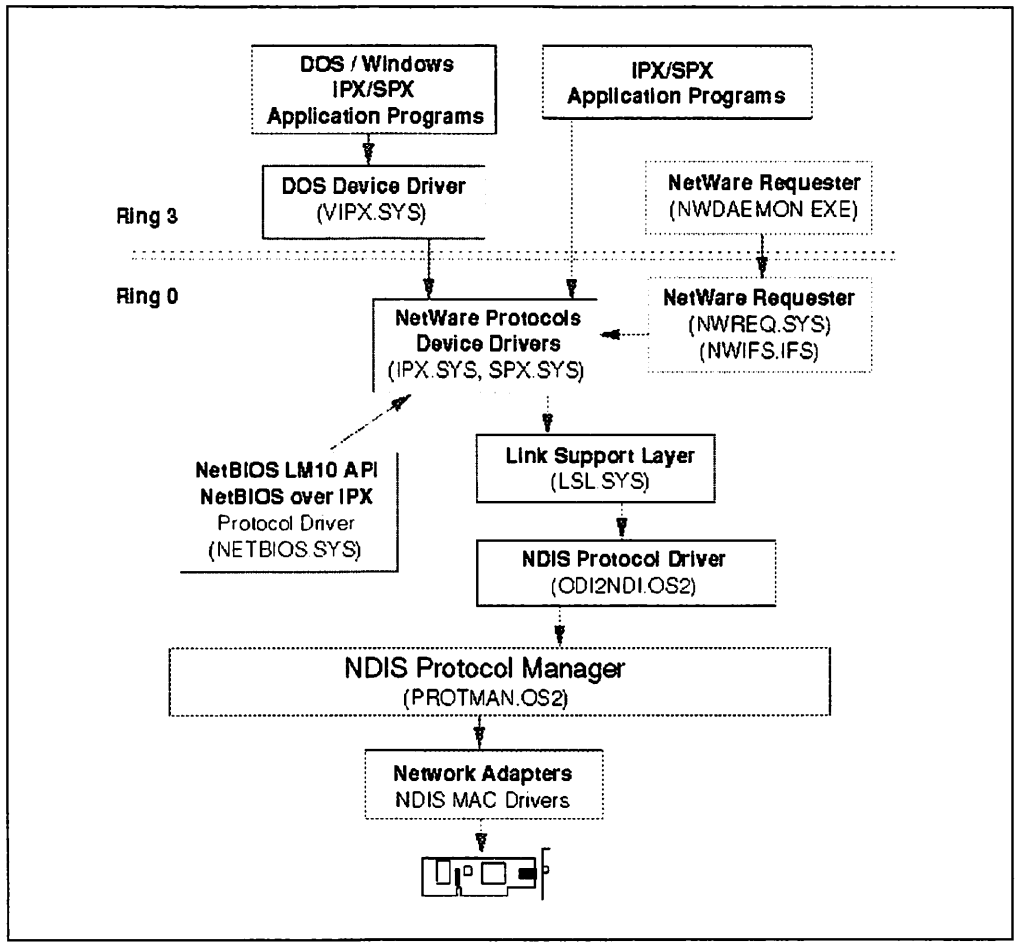


Figure 110. NetWare Requester for OS/2

Installing NetWare Requester Support on OS/2 Warp Server

When you want to install the NetWare Requester on an OS/2 Warp Server system, you have to select the NetWare File Services Gateway option on the installation panel of File and Print Sharing Services. The NetWare Requester will always need to coexist with an application which uses an NDIS protocol stack. (Unless you are doing an Easy Install and the NetWare Requester is the only LAN application that you are installing). Because of this, the OS/2 Warp Server installation will automatically install and configure the ODI2NDI driver for you.

4.6 NetWare NetBIOS Emulation

MPTS allows the configuration of Novell's NetBIOS emulator program (IPXNB) that is provided with the NetWare Requester. IPXNB provides an LM10 NetBIOS interface that may be used by workstations running NetBIOS applications that support this interface, such as File and Print Sharing Services. This capability is extremely useful for customers who have multi-segment networks connected by IPX routers or those who already use IPX as the standard protocol on their networks and do not wish to introduce additional protocols.

Figure 111 on page 160 shows an example scenario with both NetWare and NetBIOS protocols being used and NetWare Requester installed on a server. In this example, workstation A is able to access File and Print Sharing Services

resources on server B on the local LAN segment via NetBIOS, and the OS/2 Warp Server (C) on the remote LAN segment across the IPX network via IPXBEUI. In addition, it is able to use the services provided by NetWare Requester to access local and remote NetWare servers via the native IPX protocol.

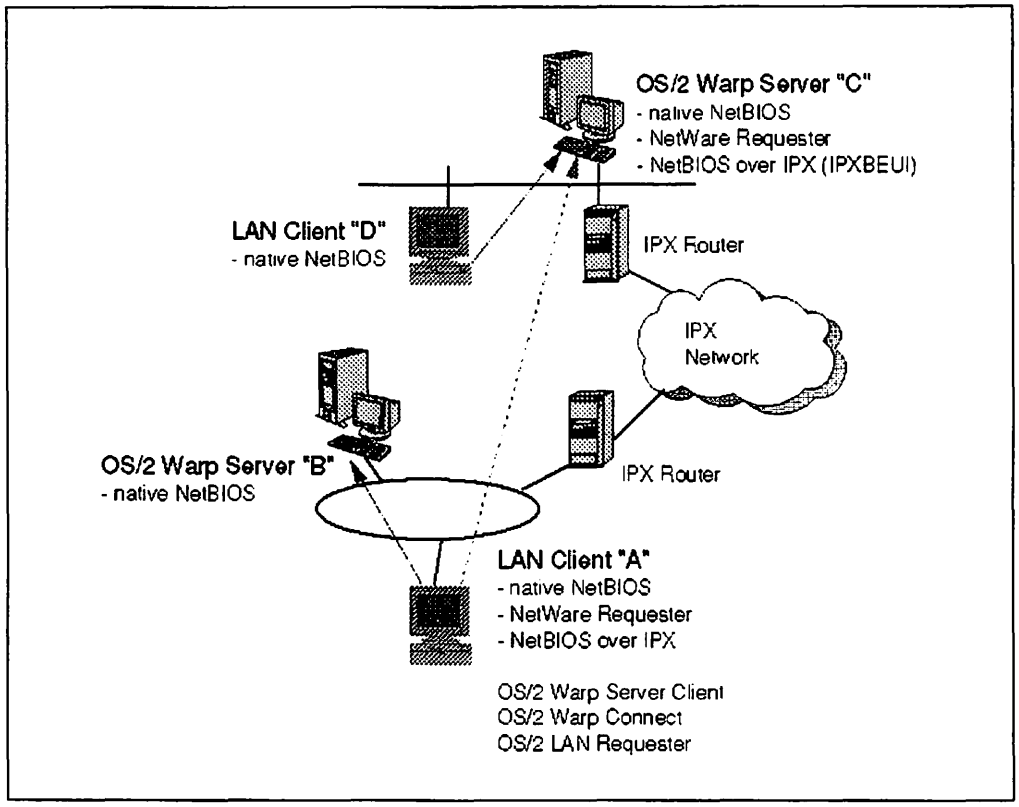


Figure 111. IPXBEUI Coexistence

Figure 112 on page 161 shows the active protocol stacks with the NetWare NetBIOS emulator loaded.

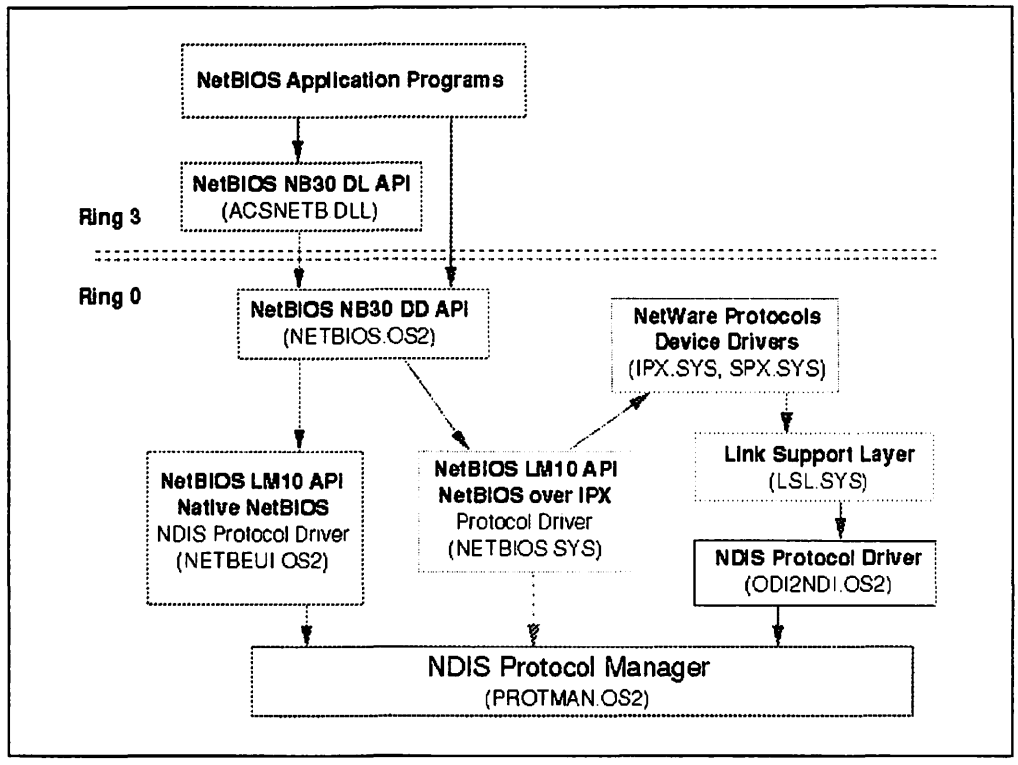


Figure 112. NetBIOS over IPX Protocol Stack

Configuring NetWare NetBIOS Emulation

The following steps are a guideline for configuring the NetWare NetBIOS emulation.

1. Install the NetWare File and Print Gateway Services with File and Print Sharing Services.
2. To configure the NetWare NetBIOS emulation, start the Install program from the NetWare File and Print Gateway Services folder.
   - Select **Configuration** and **This Workstation** (accept the default path for the NET.CFG file)
   - Select **Edit**. Figure 113 on page 162 shows the panel for configuring the NET.CFG file
   - Select **NetWare NetBIOS**

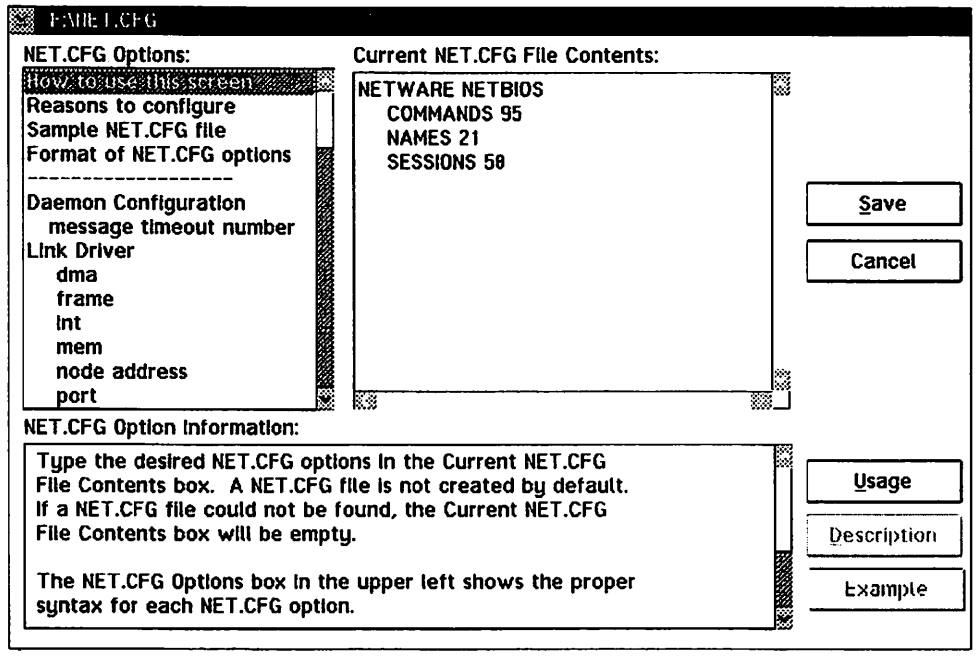


Figure 113. NetWare Requester Configuration Panel

The following NetWare NetBIOS emulation parameters determine the NetBIOS resources that are available for NetBIOS applications running over NetWare NetBIOS emulation:

- COMMANDS

  (This corresponds with the NCBS parameter in the NETBEUI_NIF section of the x:\IBMCOM\PROTOCOL.INI file - default value is 32.)
- NAMES

  (This corresponds with NAMES parameter in the NETBEUI_NIF section of the x:\IBMCOM\PROTOCOL.INI file - default value is 24.)
- SESSIONS

  (This corresponds with SESSIONS parameter in the NETBEUI_NIF section of the x:\IBMCOM\PROTOCOL.INI file - default value is 16.)

3. Make the appropriate changes to the NetBIOS resource parameters according to the amount of NetBIOS resources needed to run the NetBIOS applications.
4. Save the configuration, and close the NetWare Workstation for OS/2 Installation Utility.

   Note: If the default values for COMMANDS, NAMES and SESSIONS are adequate, you do not need to carry out this configuration of the NET.CFG file.
5. Select **Configure LAN Adapters and Protocols**. on the LAPS Configuration menu shown in Figure 101 on page 143.
6. After selecting the appropriate network adapter, the following protocols need to be configured in order to properly run the NetWare NetBIOS emulation.
   - IBM Netware Requester Support (should have been added by the installation program)
   - Netware NetBIOS Emulation over IPX - IBM Netware Requester

The IBM Netware Requester Support enables protocol stacks that comply with the Novell Open Data Link Interface (ODI) specification to operate with network adapter drivers that comply with NDIS, up to NDIS Version 2.01.

The Netware NetBIOS emulation over IPX modifies the PROTOCOL.INI file with the proper NetBIOS emulation over IPX sections in order to run NetBIOS applications over this NetBIOS emulation.

7. After LAPS configuration is complete, select **OK** to save the configuration.

Sample Configuration Files

The following changes to the CONFIG.SYS file will have been made by the configuration of the NetWare NetBIOS emulator. Note that no changes to CONFIG.SYS are made by the MPTS configuration changes.

```
  :
REM --- NetWare Requester statements BEGIN ---
SET NWLANGUAGE=ENGLISH
DEVICE=C:\NETWARE\LSL.SYS
RUN=C:\NETWARE\DDAEMON.EXE
DEVICE=C:\IBMCOM\PROTOCOL\ODI2NDI.OS2
REM -- ODI-Driver Files BEGIN --
REM -- ODI-Driver Files END --
DEVICE=C:\NETWARE\ROUTE.SYS
DEVICE=C:\NETWARE\IPX.SYS
DEVICE=C:\NETWARE\SPX.SYS
RUN=C:\NETWARE\SPDAEMON.EXE
rem DEVICE=C:\NETWARE\NMPIPE.SYS
rem DEVICE=C:\NETWARE\NPSERVER.SYS
rem RUN=C:\NETWARE\NPDAEMON.EXE
DEVICE=C:\NETWARE\NWREQ.SYS
IFS=C:\NETWARE\NWIFS.IFS
RUN=C:\NETWARE\NWDAEMON.EXE
DEVICE=C:\NETWARE\NETBIOS.SYS
RUN=C:\NETWARE\NBDAEMON.EXE
DEVICE=C:\OS2\MDOS\LPTDD.SYS
REM --- NetWare Requester statements END ---
  :
```

Figure 114. CONFIG.SYS with NetBIOS over IPX Configured (Extract)

Figure 115 on page 164 shows a PROTOCOL.INI file from a workstation with NetBIOS over IPX configured.

```
[PROT_MAN]

   DRIVERNAME = PROTMAN$

[IBMLXCFG]

   ipxnb_nif = ipxnb.nif
   odi2ndi_nif = odi2ndi.nif
   IBMTOK_nif = IBMTOK.NIF

[NETBIOS]

   DriverName = netbios$
   ADAPTER0 = ipxnb$,0

[ipxnb_nif]

   DriverName = ipxnb$
   Bindings = IBMTOK_nif

[odi2ndi_nif]

   DriverName = odi2ndi$
   Bindings = IBMTOK_nif
   NETADDRESS = "10005A88B1C9"
   TOKEN-RING = "yes"
   TOKEN-RING_SNAP = "yes"
   ETHERNET_802.3 = "no"
   ETHERNET_802.2 = "no"
   ETHERNET_II = "no"
   ETHERNET_SNAP = "no"
   TRACE = 0x0

[IBMTOK_nif]

   DriverName = IBMTOK$
   MAXTRANSMITS = 6
   RECVBUFS = 2
   RECVBUFSIZE = 256
   XMITBUFS = 1
```

Figure 115. PROTOCOL.INI with NetBIOS over IPX Configured

Figure 116 shows an extract from the IBMLAN.INI for a IBM Peer for OS/2 Version 1.0 workstation using NetBIOS over IPX.

```
[networks]

  net1 = ipxnb$,0,LM10,34,50,14
; This information is read by the redirector at device initialization time.
```

Figure 116. IBMLAN.INI Configured for NetBIOS over IPX

```
NETWARE NETBIOS
   SESSIONS=50
   COMMANDS=40
   NAMES=15
```

Figure 117. NET.CFG File for NetWare NetBIOS Emulator

Limitations When Using NetBIOS over IPX

When using NetBIOS over IPX, the following has to be considered.

An application using NetBIOS over IPX cannot communicate with another application using native NetBIOS. Even if applications are written to the NetBIOS programming interface, IPX protocol stacks cannot talk to NetBIOS protocol stacks. A partner must use the same communication protocol stack.

Performance Considerations for IPXBEUI

The NetBIOS emulation in the NetWare Requester is provided by the NETBIOS.SYS driver. The NetBIOS provided by Novell is called an emulator because it does not transmit NetBIOS packets on the network. Instead, NetBIOS packets are encapsulated in IPX packets, and the IPX packets are transmitted. The encapsulation process will impact performance of the File and Print Sharing Services. Also, bear in mind that the NetBIOS over IPX protocol does not have the same enhancements that have been specifically designed for routed networks as are available in the NetBIOS over TCP/IP protocol (see 6.4, "Reducing Broadcast Frames with TCPBEUI" on page 264).

Native NetBIOS should always be considered as the protocol of choice whenever the network configuration allows.

4.7 DOS and Windows LAN Applications on OS/2

Adapter and Protocol Services also provide virtual device drivers to allow DOS and Windows applications to use the NetBIOS and IEEE 802.2 protocol services. The device drivers are loaded, when the following statements are contained in the CONFIG.SYS file:

```
DEVICE=F:\IBMCOM\PROTOCOL\LANPDD.OS2
DEVICE=F:\IBMCOM\PROTOCOL\LANVDD.OS2
```

LANPDD.OS2 is the virtual IEEE 802.2 protocol driver, and LANVDD.OS2 is the virtual NetBIOS protocol driver for DOS and WIN-OS2 sessions. Both drivers are required to support any of these interfaces on DOS and WIN-OS2 sessions. These statements will be added by Adapter and Protocol Services automatically when you configure the NetBIOS or IEEE 802.2 protocol for at least one adapter.

To reserve NetBIOS and IEEE 802.2 resources for a DOS or WIN-OS2 session, you have to include the LTSVCFG command in the AUTOEXEC.BAT file. This command takes to following parameters:

```
LTSVCFG
   C  =     number of NetBIOS commands
   D  =     IEEE 802.2 direct station support
   N  =     number of NetBIOS names
   N1 =     NetBIOS name #1 support
   S  =     number of NetBIOS sessions
   /        separator between multiple adapter configurations
```

The resources specified with the LTSVCFG command are taken from the pool of resources that is defined in the PROTOCOL.INI file.

The *MPTS Configuration Guide* online book provides configuration and application settings examples for the virtual device drivers.

4.8 Removing Adapter and Protocol Services

Since Adapter and Protocol Services are a key feature of OS/2 Warp Server providing communications support to all other components, it cannot be removed.

4.9 Adapter and Protocol Support Related Publications

This section provides the reader with a list of selected publications for further reading on the topics discussed in this chapter.

- *MPTS Configuration Guide*, available online with OS/2 Warp Server
- *MPTS/2 Programmer's Guide*, S10H-9694
- *LAN Technical Reference IEEE802.2 and NetBIOS APIs*, SC30-3587

Chapter 5. TCP/IP Services

This chapter will describe the TCP/IP functions and services provided with OS/2 Warp Server. It is our intention to concentrate on the new Dynamic IP capabilities of TCP/IP Services rather than on basic TCP/IP functions that are also contained in this release. We will, however, provide a brief overview of base TCP/IP functions and configuration at the beginning of this chapter.

This chapter also contains a section about TCP/IP functions and services that are not included in OS/2 Warp Server, but are available from IBM as separate program products or can be purchased from other software vendors, and can be installed and used in addition to TCP/IP Services. Finally, this chapter provides examples of how OS/2 Warp Server and its TCP/IP Services can interoperate in a heterogeneous networking environment.

For a more detailed discussion of basic TCP/IP components, and for a better understanding of protocols and applications that make up the TCP/IP communication environment, please refer to 5.18, "TCP/IP Related Publications" on page 258.

5.1 Overview of TCP/IP Services

The version of TCP/IP in the OS/2 Warp Server - TCP/IP V3.1 for OS/2 - is an enhanced version from OS/2 Warp Connect. What has been added are Dynamic IP services which will be documented in detail later in this chapter. There are also add-on packages that you can install on top of OS/2 Warp Server to add NFS, X Window System and Web server capability to TCP/IP Services, which will also be explained in 5.14, "Expanding OS/2 Warp Server TCP/IP Capabilities" on page 246.

Figure 118 on page 168 shows an overview of TCP/IP Services, including functions from add-on packages. In the upper half, the TCP/IP applications, enablers and services that comprise TCP/IP Services are shown. Those applications, enablers, and services which can be added on top of TCP/IP Services show a dotted frame around the respective symbolic icon. The lower half of the figure illustrates the TCP/IP protocol stack that is supplied with OS/2 Warp Server.

As the word *stack* implies, the TCP/IP protocols can indeed be thought of as lying on top of each other because each is dependent on the function of others in that particular order. Most of the TCP/IP applications, however, require only one of the APIs, but are otherwise on the same level. We cannot show this in the diagram because the pages are not wide enough (or one would not be able to read it). There are some dependencies for applications as well:

- Ultimail requires basic SMTP functions as provided with the Sendmail application.
- NFS server requires the Portmapper application to be active in order to accept Remote Procedure Calls (RPCs).

© Copyright IBM Corp. 1996

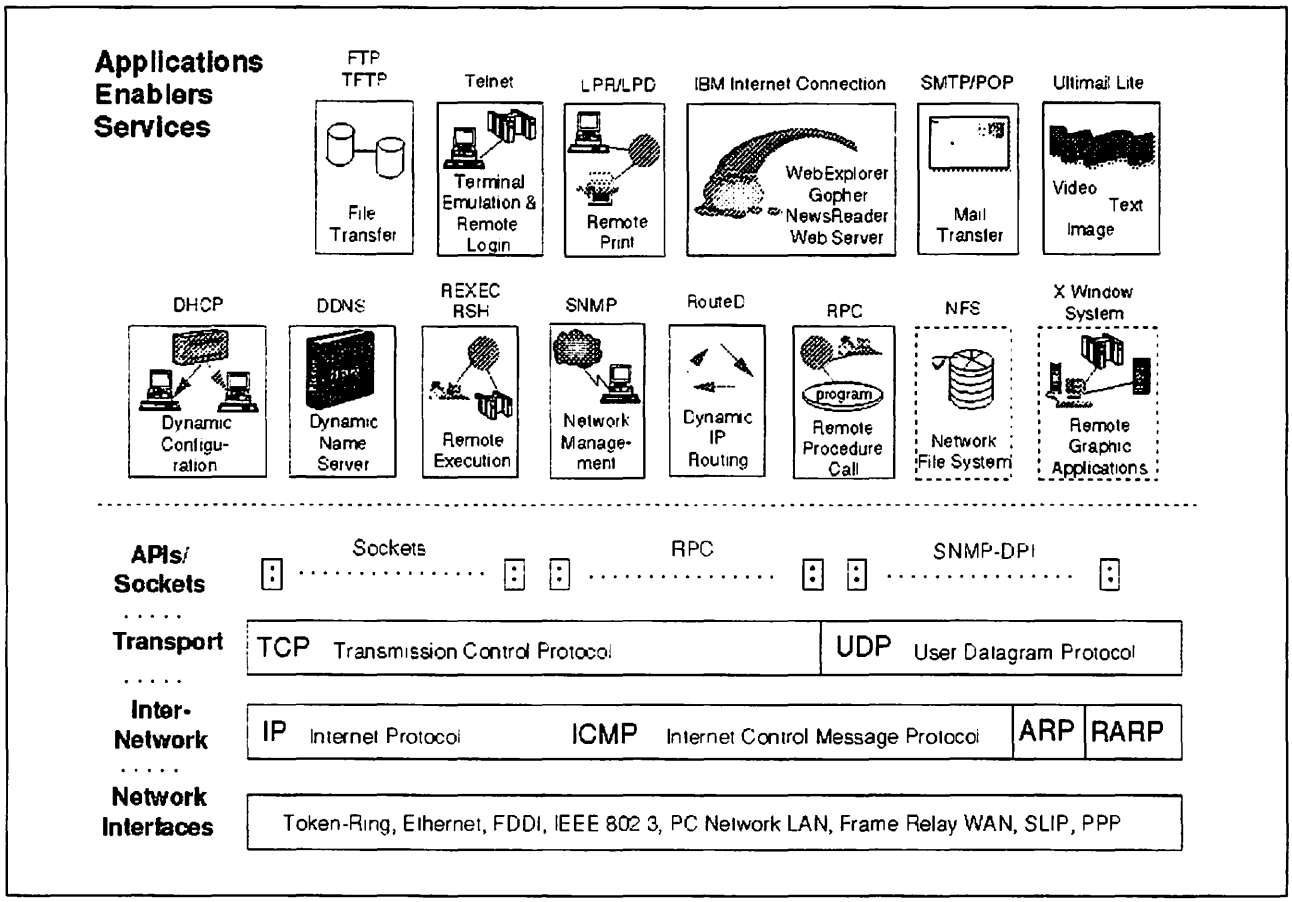


Figure 118. OS/2 Warp Server TCP/IP Services and Add-on Kits - Overview

New Functions of TCP/IP Services

The new TCP/IP functions and services that come with OS/2 Warp Server are shown in the following table:

Table 25. New Functions of TCP/IP Services

System Component	Description
Dynamic Host Configuration Protocol (DHCP) server	DHCP servers will provide the necessary information to allow DHCP clients on the network to automatically and dynamically obtain the addresses and configuration information about the network and about host operational parameters as specified by network administrators.
Dynamic Domain Name Services (DDNS) server	DDNS servers enable client hosts to dynamically register their name and address mappings in the DNS tables directly, rather than having an administrator manually perform the updates.

We will discuss those features in separate sections later in this chapter.

Basic Functions and Services of TCP/IP 3.1

The basic TCP/IP functions of TCP/IP Services include the following:

- TCP/IP protocol stack providing for simultaneous LAN and dial-up Internet access (actually contained in Adapter and Protocol Services)
- SLIP and PPP dial-up support
- Online Internet registration and utilities for dial-up users
- Remote login (Telnet, Telnet3270, Telnet5250)
- File transfer (FTP, TFTP)
- Remote program execution (Rexec, Rsh)
- Remote printing (Lpr, Lpd, LprPortD)
- Electronic mail including Multimedia support (SMTP, MIME, POP)
- Internet client services (WebExplorer, Gopher, News Reader/2)
- Network management agent (SNMPD)
- Dynamic routing of IP datagrams using the Routing Information Protocol, RIP (RouteD)
- Static automatic TCP/IP configuration at system start (Bootp)
- Useful Tools (Ping, Netstat, Iptrace, Tracerte, Finger, RPCinfo)
- REXX programming interface for Sockets and FTP APIs
- Virtual TCP/IP stack and Winsock 1.1 API for DOS and Windows applications

TCP/IP Services System Requirements

This section lists the hard disk and memory requirements for TCP/IP Services, as well as the requirements for some of the additional packages.

Fixed Disk Requirements

Table 26 shows the recommended amount of fixed disk space to hold TCP/IP Services components, as shown in the disk space indicator window during installation. These requirements are to be added to the disk space that is required for OS/2 Warp Server base (about 86MB).

Table 26 (Page 1 of 2). Fixed Disk Requirements for TCP/IP Services

Services	Required Disk (MB)
TCP/IP 3.1 Base (includes IBM Internet Connection for OS/2, Ultimedia Mail 'Lite', DOS/Windows Access)	18.4
DHCP Server	1.0
DDNS Server	1.6
Internet Connection Server	2.6
NFS Kit	1.5
NFS TCP/IP CID Install	0.3
X Window System Server Kit	12.0
X Window System Client Runtime Services	2.4
X Window System Client Programmer's Toolkit	1.5
Programmer's Toolkit	1.0

Table 26 (Page 2 of 2). Fixed Disk Requirements for TCP/IP Services	
Services	**Required Disk (MB)**
IBM Library Reader/2	1.4
Extended Networking Kit	1.0

Memory Requirements

Table 27 shows the recommended amount of memory required for some of the TCP/IP Services components. The values have been either taken from previous publications or obtained by using the THESEUS2 program, which is contained in IBM OS/2 System Performance Monitor/2 product.

Table 27. Memory Requirements for TCP/IP Services	
Services	**Recommended Memory (MB)**
OS/2 Warp Server Base, TCP/IP Protocol Stack and APIs[3]	8.0
DHCP Client	0.5
DDNS Client[2]	0.4
DHCP Server[1]	0.8 and up
DDNS Server[1]	0.9 and up
WebExplorer[1]	1.8 and up
NewsReader/2[1]	0.7 and up
Gopher[1]	0.5 and up
Ultimedia Mail 'Lite'[1]	3.7 and up
SNMPD	0.7
NFS Client[1]	0.9 and up
NFS Server (including Portmapper and PCNFSD)	1.0
Internet Connection Server[1]	1.2 and up
PMX Server[1]	2.2 and up
Internet Dialer	0.5
PPP Driver	0.5
Each other Client	at least 0.3
Each other Server	0.3 + 0.2 per Client at each Server

Notes:

1. Depending on application configuration and workload.
2. DDNS client is only running at system start, and after a DHCP address lease has been renewed.
3. This should be considered the minimum amount of RAM required to run a minimum configuration of OS/2 Warp Server with just the base operating system and TCP/IP Services installed. In general, 24MB of memory are recommended for OS/2 Warp Server.

5.2 Installing TCP/IP Services

You can choose to install TCP/IP Services when you initially install OS/2 Warp Server, or you may install TCP/IP Services later using the OS/2 Warp Server Install program which can be found in the System setup folder.

This section will describe the initial installation, starting from the OS/2 Warp Server Setup and Installation menu as shown in Figure 119.

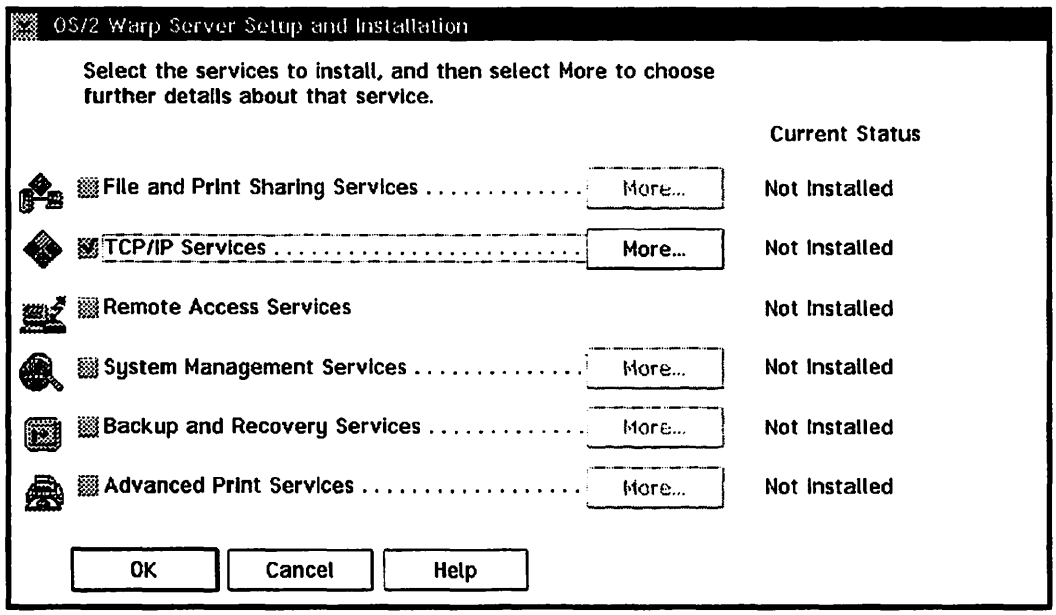


Figure 119. OS/2 Warp Server Setup and Installation Menu

On this menu, you can select the services you want to install for this OS/2 Warp Server system. Select TCP/IP Services and any other services you require. If you want to install the dynamic IP servers on this system, click on the **More** button next to TCP/IP Services. This will lead you to the following menu from which you can select the servers you want to install by clicking the respective check box.

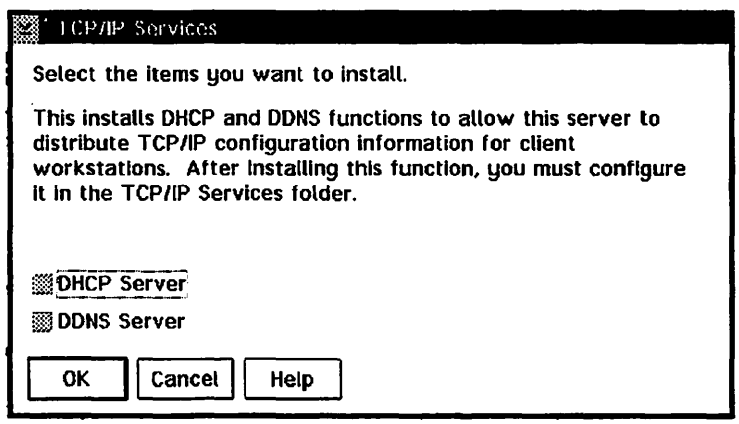

TCP/IP Services
Select the items you want to install.
This installs DHCP and DDNS functions to allow this server to distribute TCP/IP configuration information for client workstations. After installing this function, you must configure it in the TCP/IP Services folder.
DHCP Server
DDNS Server
OK
Cancel
Help

Figure 120. TCP/IP Services Installation - Dynamic IP Servers

When you have selected all services and options for this installation of OS/2 Warp Server, press **OK**. This will lead you to the Configuration menu where you

can configure any services of OS/2 Warp Server that you have previously selected to be installed. A red arrow indicates that additional configuration is needed for a service. The left side of this menu has the layout of a directory tree, allowing you to move up and down the tree during configuration. Entries that apply to more than one service should be automatically updated if you make changes anywhere in the tree.

Go to the TCP/IP Services entry in the tree. On the right side of the menu, you have to enter the configuration parameters required for installation, as shown in Figure 121.

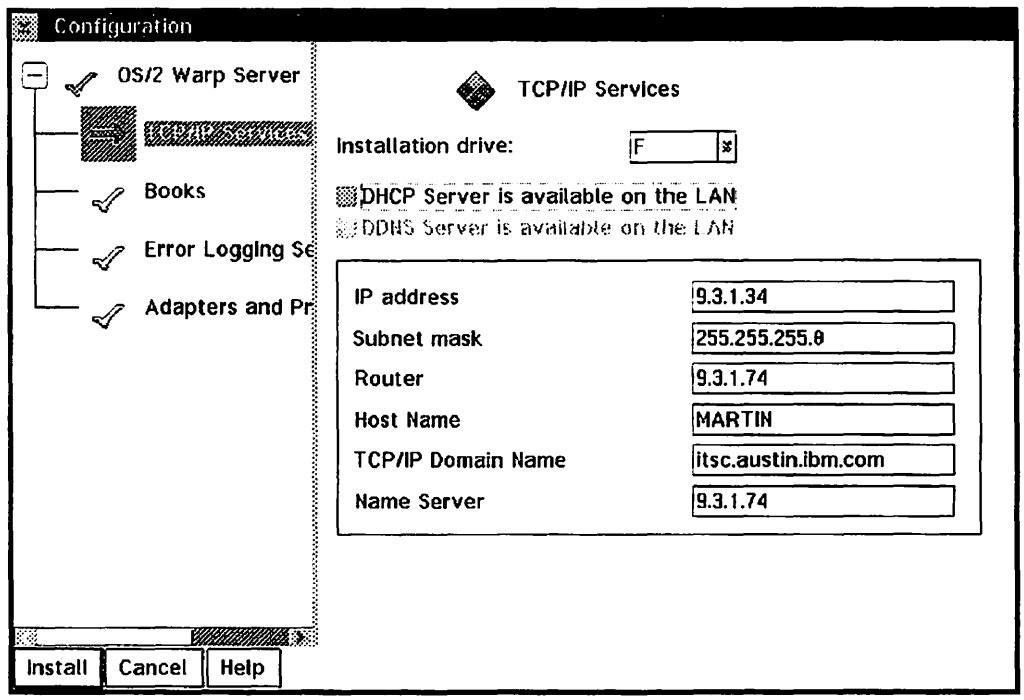


Figure 121. TCP/IP Services Initial Configuration

The following table summarizes the configuration parameters of this menu and describes their purposes.

- If you want to use the new Dynamic IP components to make the configuration easier for you, check the DHCP and DDNS server boxes, and enter a hostname.
- If you want to configure TCP/IP manually, do not check the DHCP and DDNS boxes, and fill in all the other fields according to the information you have been given by your network coordinator.

Note: When you selected to install the DHCP server you cannot use DHCP to automatically configure TCP/IP on this system. Though the DHCP and DDNS client programs will be installed with Adapter and Protocol Services, they should not be used on a system that runs the DHCP server.

Table 28 (Page 1 of 2). TCP/IP Services Initial Configuration

Configuration Item	Configuration Data
Installation Drive	Select a drive on which to install TCP/IP Services.

Table 28 (Page 2 of 2). TCP/IP Services Initial Configuration	
Configuration Item	**Configuration Data**
DHCP Server is active on the LAN	Check, if you want the DHCP client to automatically configure this interface with parameters obtained from a DHCP server, if one exists on the network.
DDNS Server is active on the LAN	Check, if you also want the DDNS to specify a hostname and/or update a DDNS server with that information, if one exists on the network.
IP Address	The IP address of this interface to the IP network
Subnet Mask	This is the value obtained from your network coordinator to define the network range of your IP address.
Router	Enter the IP address of a host that will act as your default IP router.
Host Name	Enter a name that you wish to use with this system.
TCP/IP Domain Name	Enter the name for the TCP/IP domain to which this system will belong.
Name Server	Enter the IP address of a name server for the TCP/IP domain to which this system will belong.

You may want to verify that the TCP/IP protocol stack is indeed installed for your LAN adapter(s) after you have finished the basic configuration for TCP/IP Services. To do so, go to the Adapter and Protocol Services entry in the tree, and check the selected adapters and protocols. Please see Chapter 4, "Adapter and Protocol Services" on page 125 for more information about the installation and configuration of Adapter and Protocol Services.

5.3 Additional Configuration for TCP/IP Services

After the installation of OS/2 Warp Server has completed, you will find two folders on your OS/2 Desktop which are related to TCP/IP Services:

1. TCP/IP folder
2. IBM Internet Connection for OS/2 folder

Those folders contain icons for TCP/IP applications as well as online documentation. To start a TCP/IP application, simply double-click the appropriate icon. The applications contained in the Internet Connection folder are the same as the ones in the TCP/IP folder. The difference is that any application which is started from the Internet Connection folder will invoke the Internet Dialer program in order to dial up to your Internet service provider before you can actually use the application. Figure 122 on page 174 shows the TCP/IP folder.

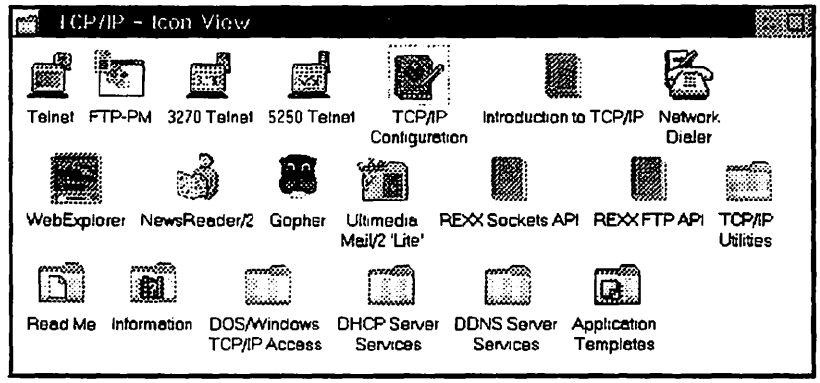


Figure 122. TCP/IP Folder

Figure 123 shows the Internet Connection folder.

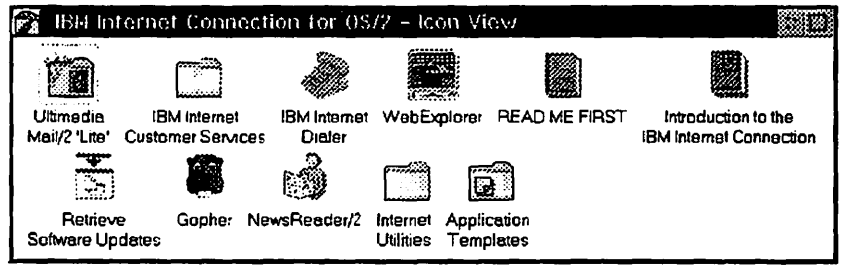


Figure 123. IBM Internet Connection for OS/2 Folder

To make changes to your TCP/IP configuration or to configure services that have not been configured during installation, start the TCP/IP Configuration program by double-clicking its icon on the TCP/IP folder. This will open a configuration notebook which holds all TCP/IP Services configuration parameters.

Configure Network Interfaces

Figure 124 on page 175 shows the first page of this notebook, the Configure Network Interface Parameters page. On this page, you can configure the TCP/IP network interfaces of your OS/2 Warp Server system.

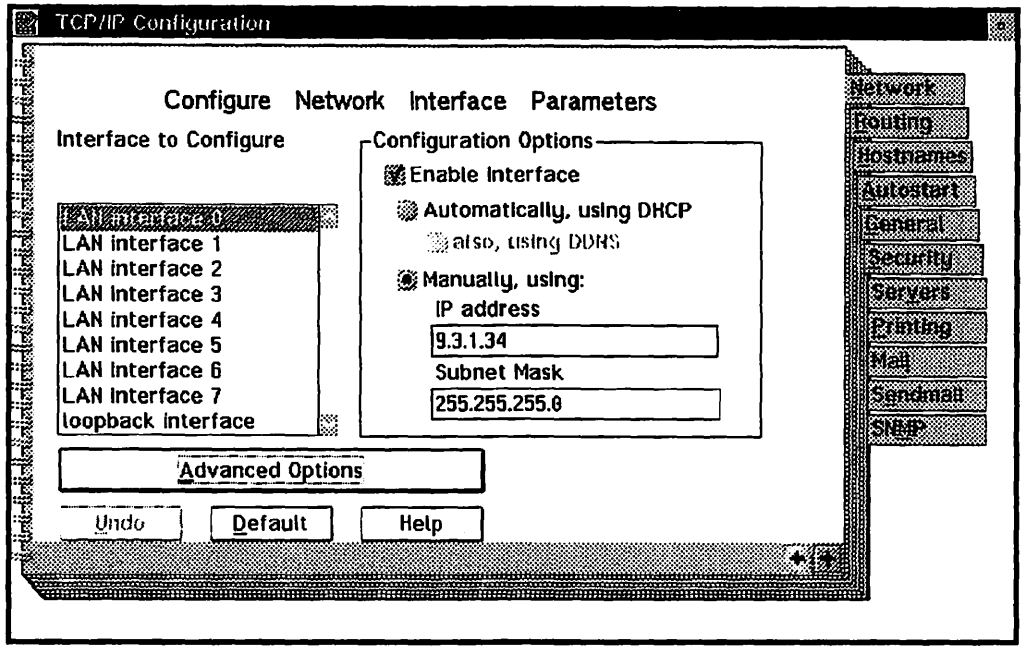


Figure 124. TCP/IP Services Configuration Notebook - Configure Network Interface Parameters

The following table summarizes the configuration parameters of this page and describes their purposes.

Table 29. TCP/IP Services Configuration Notebook - Network Page	
Configuration Item	**Configuration Data**
Interface to Configure	Select an interface to configure for use by TCP/IP Services.
Enable interface	Check, if you want to activate a selected interface.
Automatically, using DHCP	Check, if you want the DHCP client to automatically configure this interface with parameters obtained from a DHCP server, if one exists on the network.
also, using DDNS	Check, if you also want the DDNS to specify a hostname and/or update a DDNS server with that information, if one exists on the network.
Manually, using:	Check, if you want to configure a selected interface manually. In this case, you are using neither DHCP not DDNS.
IP address	The IP address of this interface to the IP network.
Subnet mask	This is the value obtained from your network coordinator to define the network range of your IP address.
Advanced Options	Check, if you want to configure additional parameters as shown in the following figure.

Figure 125 on page 176 shows the Advanced Options menu for network interfaces.

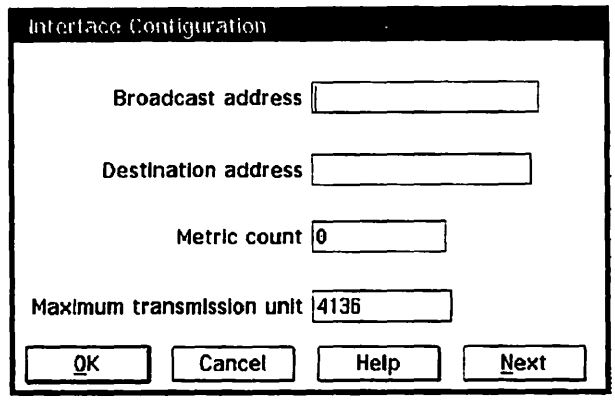


Figure 125. TCP/IP Services Network Interfaces - Advanced Options

The following table summarizes the configuration parameters of this menu and describes their purposes.

Table 30. TCP/IP Services Network Interfaces - Advanced Options

Configuration Item	Configuration Data
Broadcast address	The broadcast address for your IP network, derived from the combination of your IP address and subnet mask. This will be calculated automatically by TCP/IP, so you do not need to specify it.
Destination address	The base address of your IP network, derived from the combination of your IP address and subnet mask. This will be calculated automatically by TCP/IP, so you do not need to specify it.
Metric count	The number of hops that can be used to access another IP address.
Maximum transmission unit	Specify the maximum IP packet size for that interface. The default is 1500 bytes.

Figure 126 on page 177 shows the Interface Configuration menu for network interfaces. You can get to that menu by clicking on the **Next** button in the Advanced Options menu.

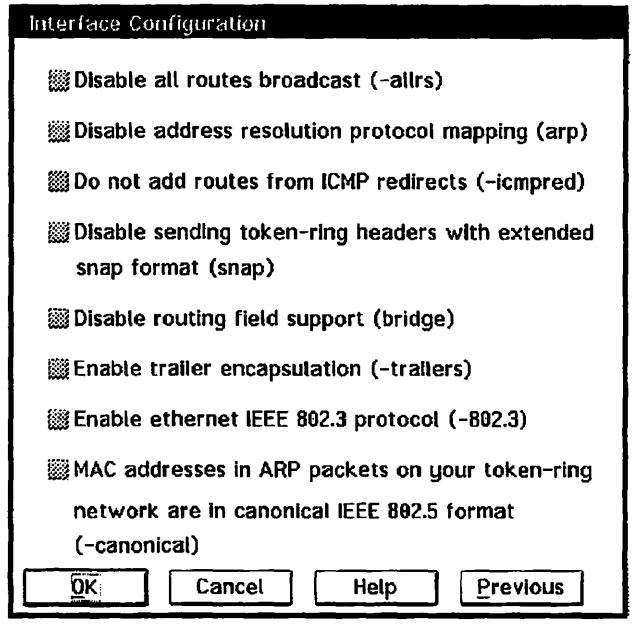

Interface Configuration
Disable all routes broadcast (-allrs)
Disable address resolution protocol mapping (arp)
Do not add routes from ICMP redirects (-icmpred)
Disable sending token-ring headers with extended snap format (snap)
Disable routing field support (bridge)
Enable trailer encapsulation (-trailers)
Enable ethernet IEEE 802.3 protocol (-802.3)
MAC addresses in ARP packets on your token-ring network are in canonical IEEE 802.5 format (-canonical)
OK
Cancel
Help
Previous

Figure 126. TCP/IP Services Network Interfaces - Interface Configuration

The following table summarizes the configuration parameters of this menu and describes their purposes.

Table 31. TCP/IP Services Network Interfaces - Interface Configuration

Configuration Item	Configuration Data
Disable all routes broadcast (-allrs)	Use this field to set the token ring broadcast indicator. All-Routes broadcast (allrs) is a default.
Disable address resolution protocol mapping (arp)	Use this field to set the use of the Address Resolution Protocol (ARP) for mapping between IP addresses and LAN adapter addresses. Default is enabled.
Do not add routes from ICMP redirects (-icmpred)	Use this field to allow or deny TCP/IP to add routes obtained by ICMP redirects.
Disable sending token-ring headers with extended snap format (snap)	Use this field to send TCP/IP packets with headers that have the extended SNAP header format.
Disable routing field support (bridge)	Use this field to enable source routing information in token-ring packets.
Enable trailer encapsulation (-trailers)	Use this field to request the use of a trailer link level encapsulation when sending messages.
Enable Ethernet IEEE 802.3 protocol (-802.3)	Use this field to disable Ethernet 802.3 and enable Ethernet DIX2.
MAC address in ARP packets on your token-ring network are in canonical IEEE 802.5 format (-canonical)	Use this field to indicate that MAC addresses in the Address Resolution Protocol (ARP) packet on this token-ring network are in the canonical IEEE 802.5 form.

These configuration items are added as parameters to the IFCONFIG command that initializes a TCP/IP interface.

Click on **OK** to finish the TCP/IP interface configuration.

Configure Routers

Figure 127 shows the Configure Routing Information page of the configuration notebook. On this page, you can configure TCP/IP routing information for your OS/2 Warp Server system.

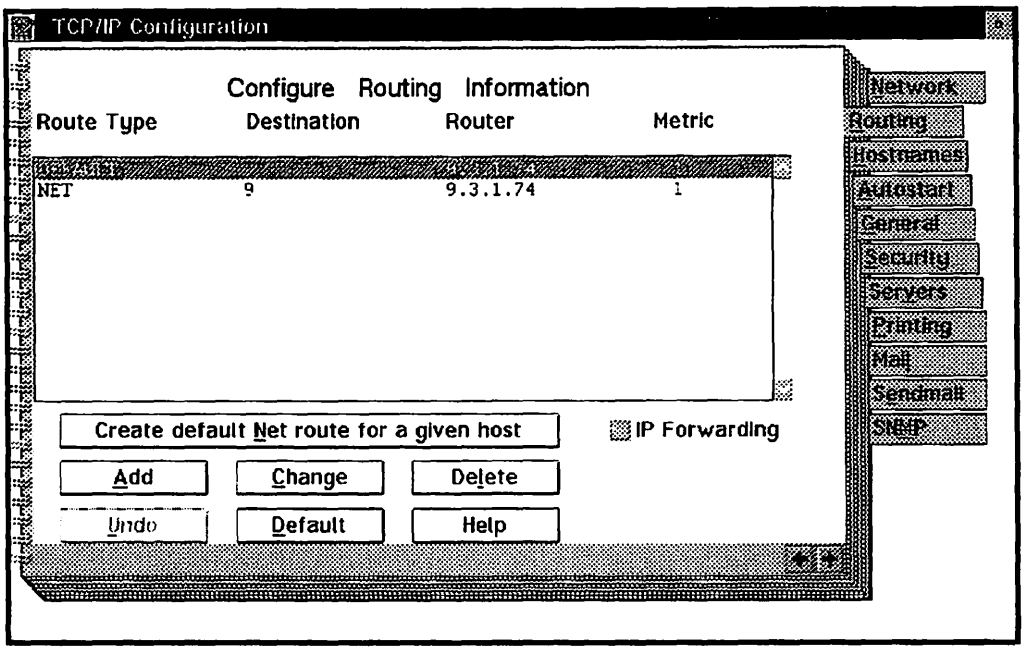


Figure 127. TCP/IP Services Configuration Notebook - Configure Routing Information

The list shows the characteristics of existing routes, if there are any. The following table summarizes the configuration parameters of this page and describes their purposes.

Table 32. TCP/IP Services Configuration Notebook - Routing Page

Configuration Item	Configuration Data
Create default Net route for a given host	If you plan to simultaneously use TCP/IP through a LAN connection and the Internet Connection Kit through a service provider, select this option to have TCP/IP calculate the route needed to access specific hosts.
IP Forwarding	Check, if you want this machine to act as an IP router. If you have only one active IP interface, this parameter will be ignored.

You can add, change and delete entries from this list, as you require.
Figure 128 on page 179 shows the Add Route Entry menu of the Routing page.

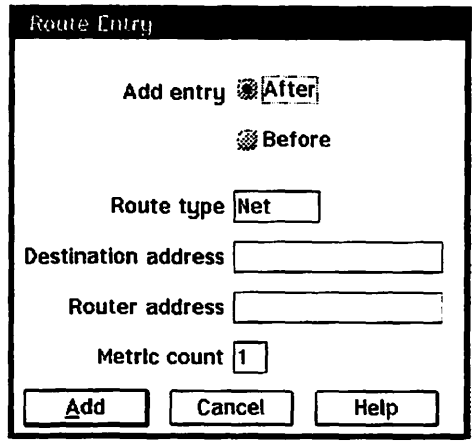


Figure 128. TCP/IP Services Routing Page - Add Route Entry

The following table summarizes the configuration parameters of this menu and describes their purposes.

Table 33. TCP/IP Services Routing Page - Add Route Entry

Configuration Item	Configuration Data
Add entry	Select whether to add the entry before the currently marked entry in the list, or after that.
Route type	Specify the type of route you want to add: • Default • Net • Subnet • Host
Destination address	The IP address of the destination network, subnet, or host to which you require to send IP datagrams. **Note:** This field is not required for default routes.
Router address	The IP address of the router on your IP subnet which provides a route to the specified destination.
Metric count	The number of hops, or intermediate routers, to the specified destination. A number of 16 or above indicates that this destination cannot be reached.

Configure Hostnames and Nameservers

Figure 129 on page 180 shows the Configure LAN Name Resolution Services page of the configuration notebook. On this page, you can specify the Domain Name System parameters for your OS/2 Warp Server system.

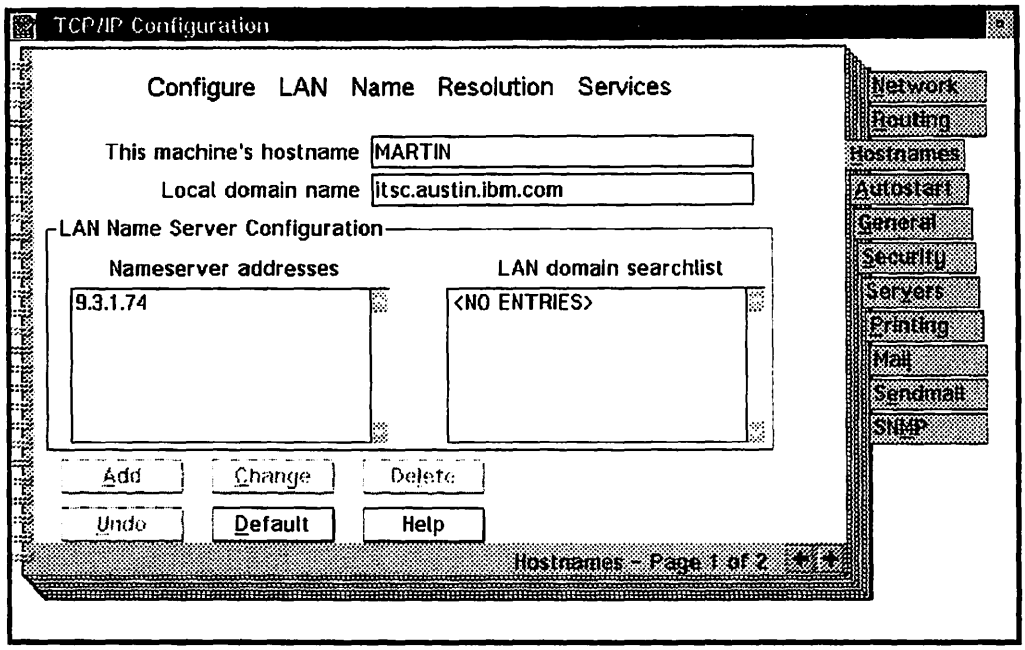


Figure 129. TCP/IP Services Configuration Notebook - Configure LAN Name Resolution Services

The following table summarizes the configuration parameters of this page and describes their purposes.

Table 34. TCP/IP Services Configuration Notebook - Hostnames Page 1

Configuration Item	Configuration Data
This machine's hostname	The name of your OS/2 Warp Server system by which it will be known in the IP Domain Name System (DNS).
Local domain name	The name of the IP domain to which this system belongs.
LAN Nameserver addresses	The IP address(es) of domain nameserver(s) on the LAN. **Note:** You will have to specify a domain nameserver for each dial-up connection that you want to use, for instance with the Internet Connection Kit. Each of those nameserver addresses will be different from the nameserver that you use on the LAN connection.
LAN domain searchlist	Domain names to be searched when an application issues a request using only a hostname.

Figure 130 on page 181 shows the Configure Name Resolution Services page of the configuration notebook. On this page, you can specify the Domain Name System parameters for your OS/2 Warp Server system.

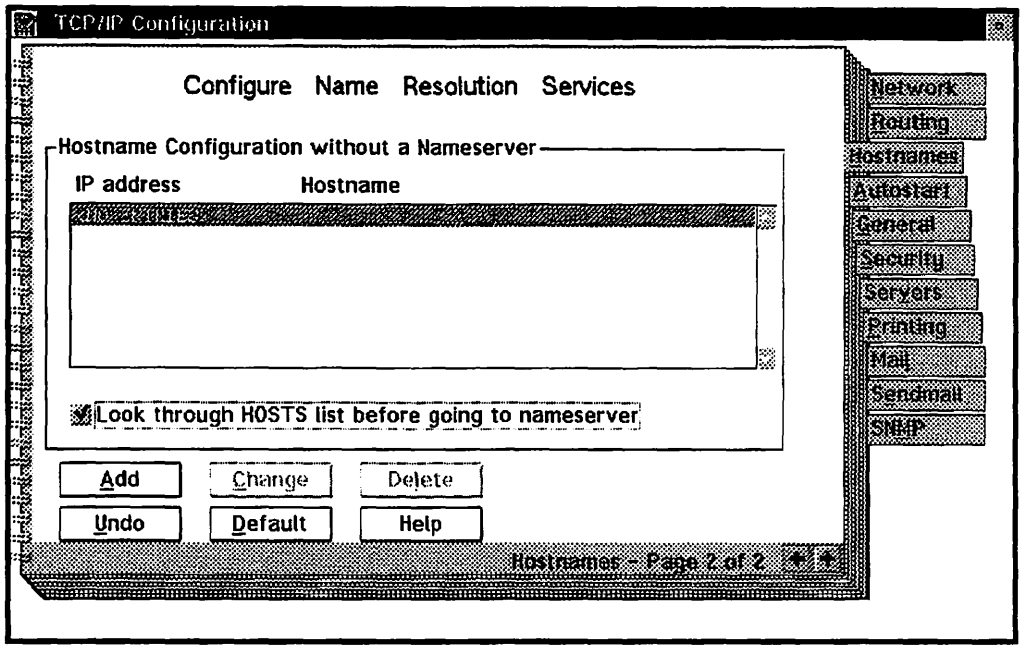


Figure 130. TCP/IP Services Configuration Notebook - Configure Name Resolution Services

The list shows the contents of an existing HOSTS list. The following table summarizes the configuration parameters of this page and describes their purposes.

Table 35. TCP/IP Services Configuration Notebook - Hostnames Page 2

Configuration Item	Configuration Data
Look through HOSTS list before going to nameserver	Check this box if you want the local resolver to look up the \MPTN\ETC\HOSTS file to resolve hostnames to IP addresses, before it contacts a domain nameserver. This will prevent time-out delays if a nameserver is no longer available. It will also be useful if you are using a dial-up connection, since that may replace the nameserver information while it is operative. This setting will be stored in the OS/2 environment variable USE_HOSTS_FIRST.

You can add, change and delete entries from this list, as you require. Figure 131 on page 182 shows the Hosts Entry menu of the Routing page.

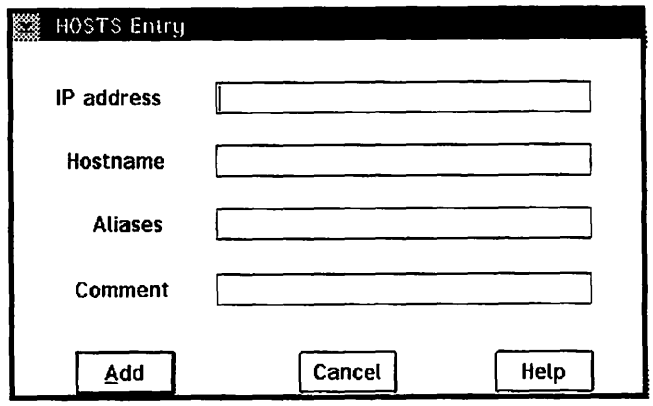


Figure 131. TCP/IP Services Hostnames Page 2 - Hosts Entry

The following table summarizes the configuration parameters of this menu and describes their purposes.

Table 36. TCP/IP Services Hostnames Page 2 - Add Hosts Entry

Configuration Item	Configuration Data
IP address	The IP address of another system.
Hostname	The name by which that host will be known to applications on your system. This can be a combination of hostname and domain name.
Aliases	An optional nickname for that host.
Comment	An optional comment for that entry.

Configure Services for Autostart

Figure 132 shows the Configure Automatic Starting of Services page of the configuration notebook. On this page, you can select TCP/IP services and applications you want to start automatically with OS/2 Warp Server.

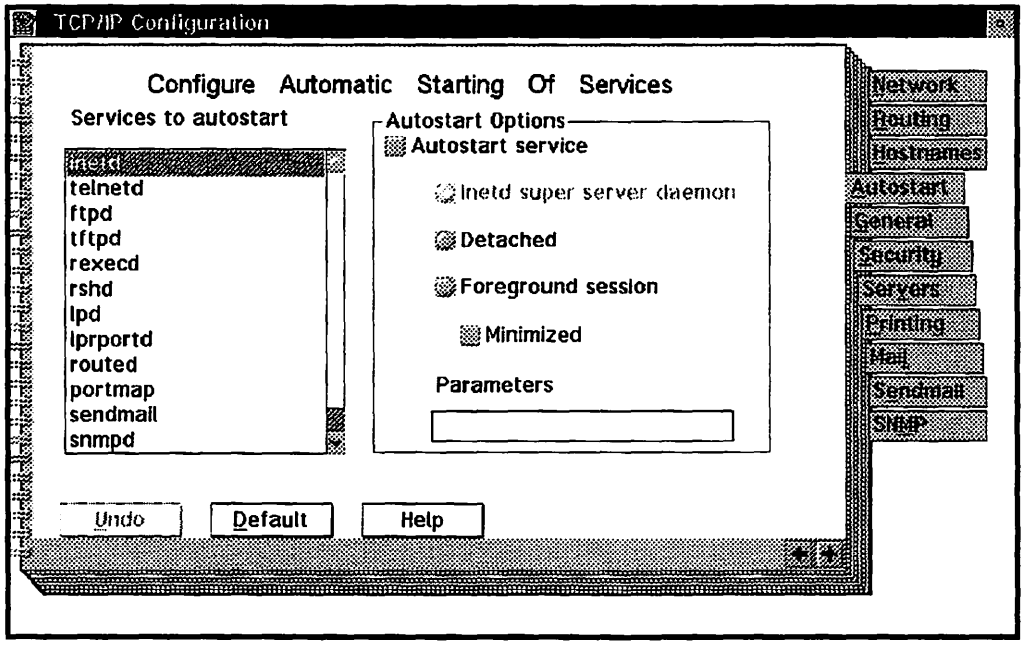


Figure 132. TCP/IP Services Configuration Notebook - Configure Automatic Starting of Services

The following table summarizes the configuration parameters of this page and describes their purposes.

Table 37. TCP/IP Services Configuration Notebook - Autostart Page

Configuration Item	Configuration Data
Services to autostart	Select one or more services which you want to be started when you turn your computer on, or after you reboot OS/2 Warp Server.
Autostart service	Check this box, if you actually want to autostart a selected service.
Inetd super server daemon	Select this option, if you want one or more services to be started within a single program. This will prevent your desktop from becoming too crowded (or your task list from becoming too long).
Detached	Select this option, if you want to run the service as a detached OS/2 process. This may not be a good selection, if you want to stop the service other than to reboot your system (or use the process manager from Systems Management Services to kill this service). It may be a good selection for programs such as lprportd.
Foreground session	Select this option, if you want to run the service as an OS/2 session in the foreground.
Minimized	Select this option, if you want to run the service in a minimized OS/2 window.
Parameters	Specify optional parameters for a selected service. **Note:** You can only pass parameters to a service, if it is *not* stated through inetd.

Configure General Parameters

Figure 133 on page 184 shows the Configure General Parameters page of the configuration notebook. On this page, you can configure general parameters that apply to several components of TCP/IP Services.

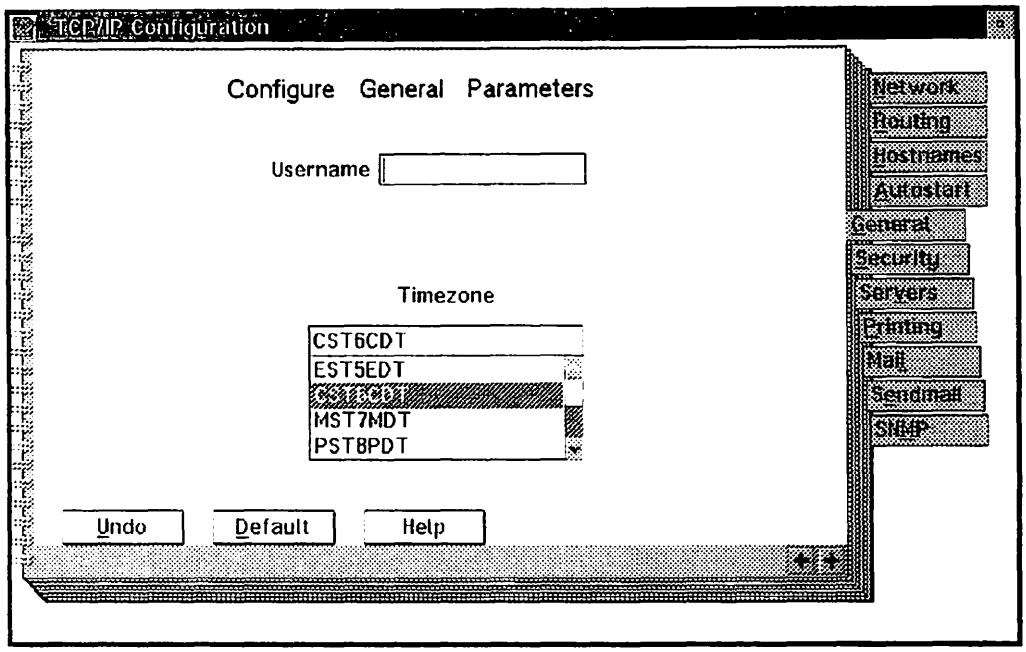


Figure 133. TCP/IP Services Configuration Notebook - Configure General Parameters

The following table summarizes the configuration parameters of this page and describes their purposes.

Table 38. TCP/IP Services Configuration Notebook - General Page

Configuration Item	Configuration Data
Username	Specify the name for a user who is authorized to execute commands in your system by using REXEC. This name will also be used by the LPR client on your system to identify print jobs that you send to a TCP/IP printer. This setting will be stored in the OS/2 environment variable USER.
Timezone	The time zone of the location where your system is installed. This is important to preserve time stamps for files in file sharing environments, such as NFS.

Configure Access Security

Figure 134 on page 185 shows the first Configure Server Security page of the configuration notebook. On this page, you can configure access control for your OS/2 Warp Server system when using TCP/IP Services.

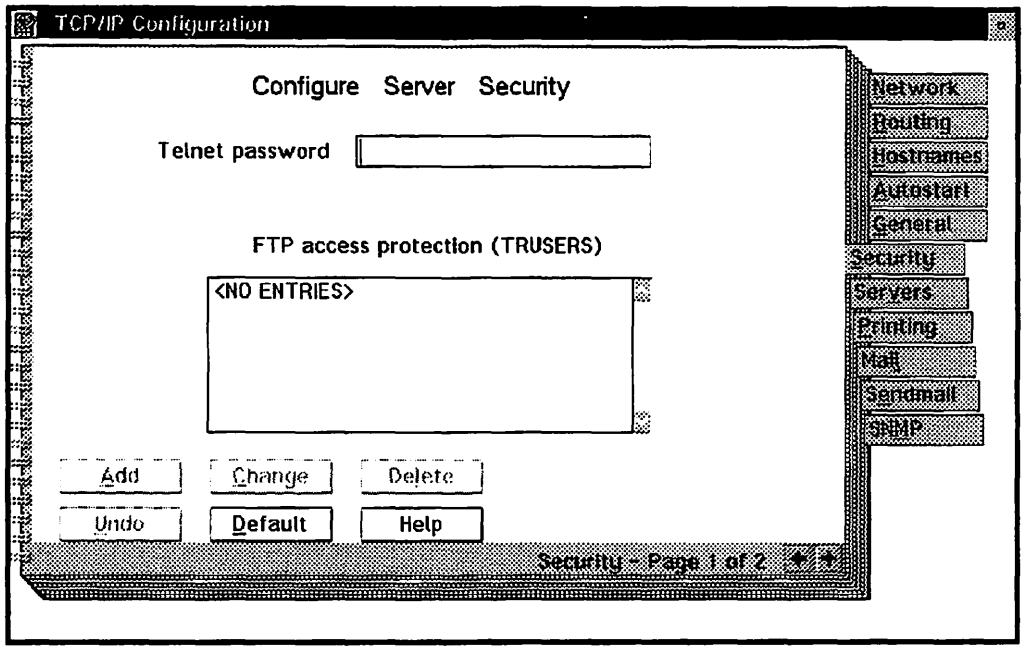


Figure 134. TCP/IP Services Configuration Notebook - Configure Server Security Page 1

The following table summarizes the configuration parameters of this page and describes their purposes.

Table 39. TCP/IP Services Configuration Notebook - Security Page 1

Configuration Item	Configuration Data
Telnet password	The password string which remote users have to use in order to connect to the Telnet server on your system. This setting will be stored in the OS/2 environment variable `TELNET.PASSWORD.ID`.

Note: Enabling this implementation of Telnet access can be dangerous, because once a user has received the password information for your system, rightfully or not, he or she can access every file and directory in your system.

Use the FTP access protection menu to configure FTP authorization. The list shows the contents of an existing TRUSERS (trusted users) file. You can add, change and delete entries from this list, as you require. Figure 135 on page 186 shows the FTP User Entry menu of the Security page 1.

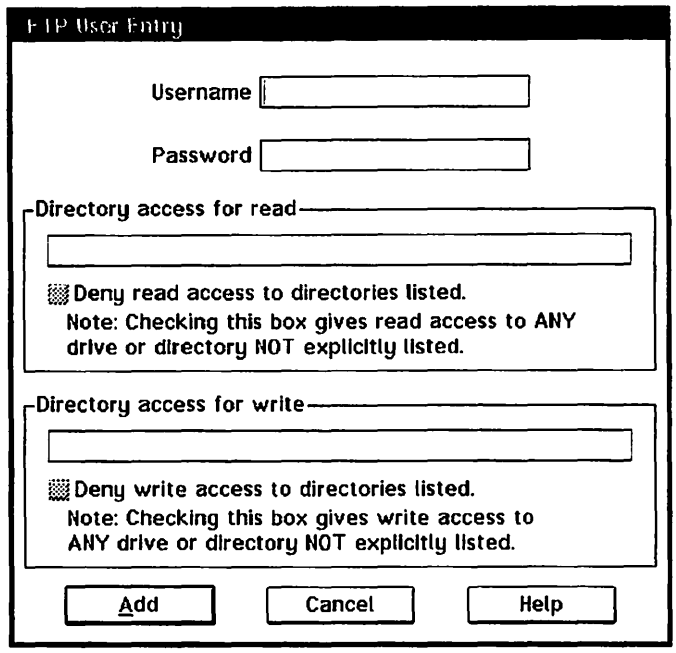

FTP User Entry
Username
Password
Directory access for read
Deny read access to directories listed.
Note: Checking this box gives read access to ANY drive or directory NOT explicitly listed.
Directory access for write
Deny write access to directories listed.
Note: Checking this box gives write access to ANY drive or directory NOT explicitly listed.
Add
Cancel
Help

Figure 135. TCP/IP Services Security Page 1 - FTP User Entry

The following table summarizes the configuration parameters of this menu and describes their purposes.

Table 40. TCP/IP Services Security Page 1 - FTP User Entry

Configuration Item	Configuration Data
Username	The name of a remote user.
Password	The password for that remote user. **Note:** Every user requires a password, except the user *anonymous*.
Directory access for read	Specify the directories to which that use will be allowed read access. Separate multiple entries with blanks.
Deny read access to directories listed	Check here, if you want to deny read access to the directories listed above. That would imply that the user has read access to all directories that are not listed.
Directory access for write	Specify the directories to which that use will be allowed write access. Separate multiple entries with blanks.
Deny write access to directories listed	Check here, if you want to deny write access to the directories listed above. That would imply that the user has write access to all directories that are not listed.

Figure 136 on page 187 shows the second Configure Server Security page of the configuration notebook. On this page, you can configure access control for your OS/2 Warp Server system when using TCP/IP Services.

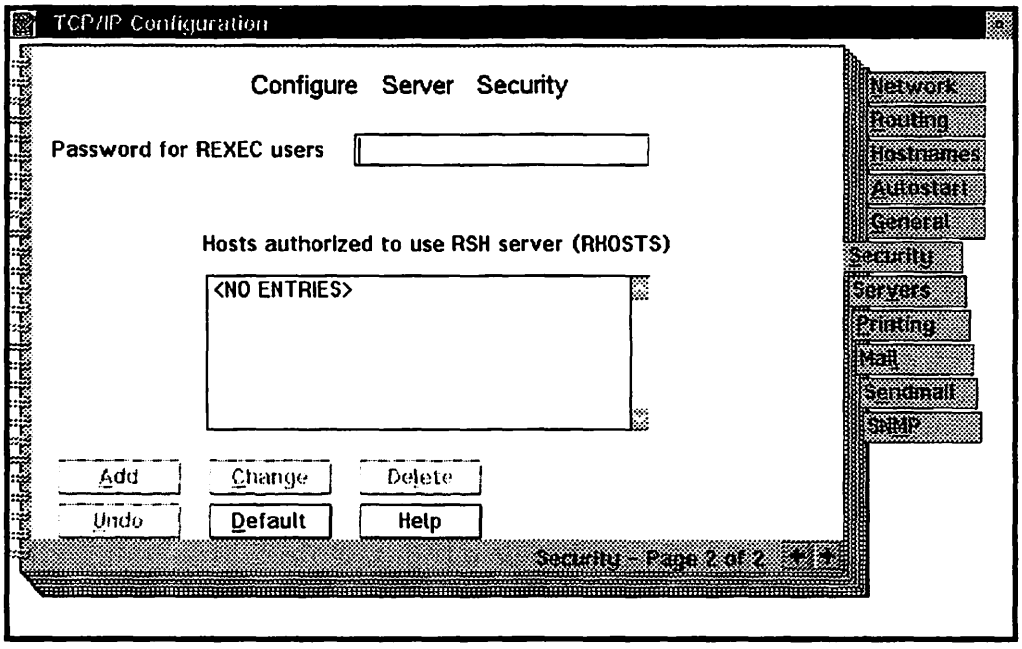


Figure 136. TCP/IP Services Configuration Notebook - Configure Server Security Page 2

The following table summarizes the configuration parameters of this page and describes their purposes.

Table 41. TCP/IP Services Configuration Notebook - Security Page 2

Configuration Item	Configuration Data
Password for REXEC users	The password string which remote users have to use in order to connect to the REXEC server on your system. This setting will be stored in the OS/2 environment variable PASSWD.

Use the Hosts authorized to use RSH server (RHOSTS) menu to configure RSH access control. The list shows the contents of an existing RHOSTS (remote hosts) file. You can add, change and delete entries from this list, as you require. Figure 137 shows the RHOSTS Entry menu of the Security page 2.

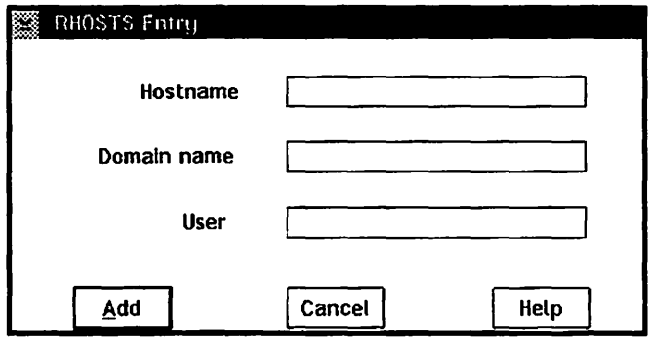


Figure 137. TCP/IP Services Security Page 2 - RHOSTS Entry

The following table summarizes the configuration parameters of this menu and describes their purposes.

Table 42. TCP/IP Services Security Page 2 - RHOSTS Entry	
Configuration Item	**Configuration Data**
Hostname	The name of a host from which users can connect to the RSH server on your system.
Domain name	The domain name of that host.
User	The name of a user on that host who is actually allowed to use the RSH server on your system. If no name is specified, any user on that host can connect to your RSH server.

Configure Internet Servers

Figure 138 shows the Configure Servers for Applications page of the configuration notebook. On this page, you can configure servers that you want to access from your OS/2 Warp Server system when using TCP/IP Services.

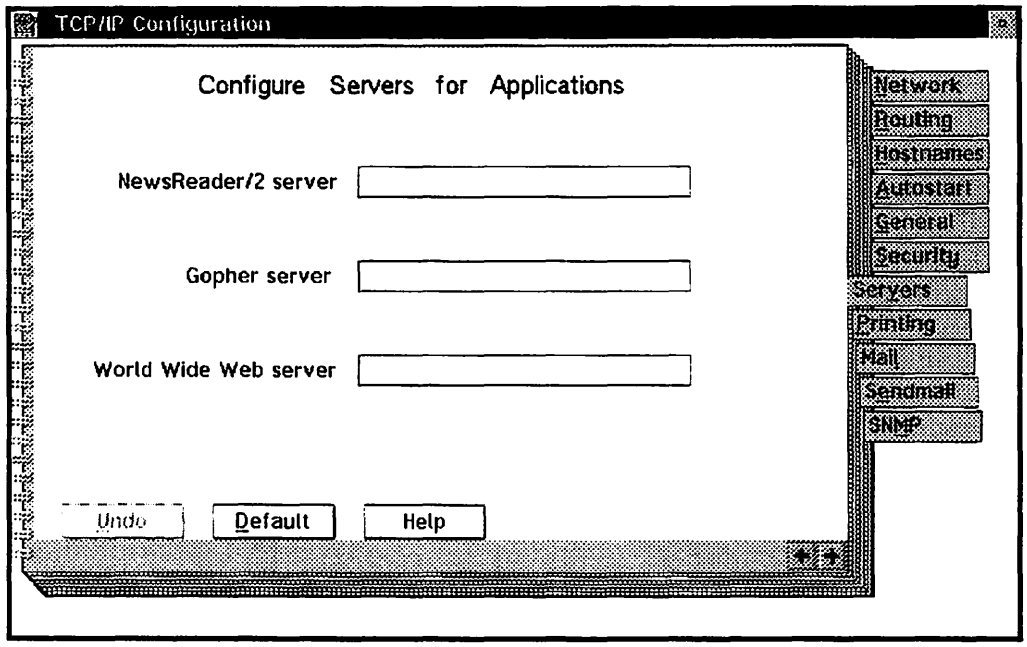


Figure 138. TCP/IP Services Configuration Notebook - Configure Servers for Applications

The following table summarizes the configuration parameters of this page and describes their purposes.

Table 43. TCP/IP Services Configuration Notebook - Servers Page	
Configuration Item	**Configuration Data**
NewsReader/2 server	The hostname or IP address of a news server that you want to use.
Gopher server	The hostname or IP address of a gopher server that you want to use.
World Wide Web server	The hostname or IP address of a WWW server that you want to use.

Configure Remote Printing

Figure 139 shows the Configure Printing Services page of the configuration notebook. On this page, you can configure parameters for remote TCP/IP printing with your OS/2 Warp Server system.

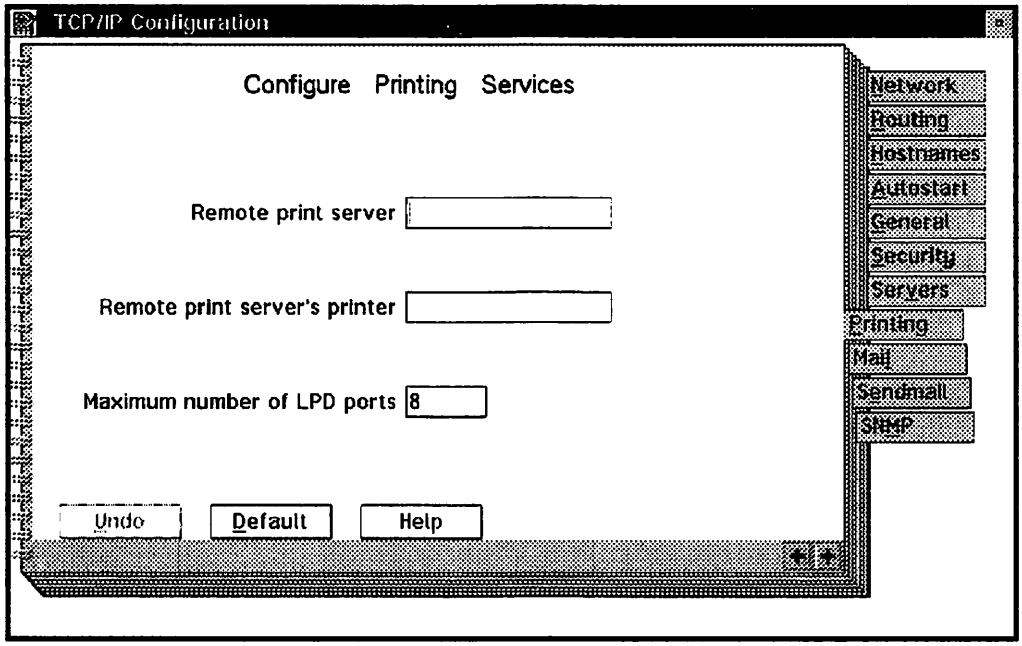


Figure 139. TCP/IP Services Configuration Notebook - Configure Printing Services

The following table summarizes the configuration parameters of this page and describes their purposes.

Table 44. TCP/IP Services Configuration Notebook - Printing Page

Configuration Item	Configuration Data
Remote print server	The hostname of a TCP/IP print server. This setting will be stored in the OS/2 environment variable LPR_SERVER.
Remote print server's printer	The name of the print queue or device on the print server. This setting will be stored in the OS/2 environment variable LPR_PRINTER.
Maximum number of LPD ports	The number of port objects that will be available when you create an OS/2 printer object for a TCP/IP printer. **Note:** LPRPORTD must be running before an application can print to those printers.

Configure Ultimail Lite

Figure 140 on page 190 shows the Configure Mail for Ultimail or Mailing from NewsReader/2 page of the configuration notebook. On this page, you can configure the environment for Multimedia mail when using TCP/IP Services.

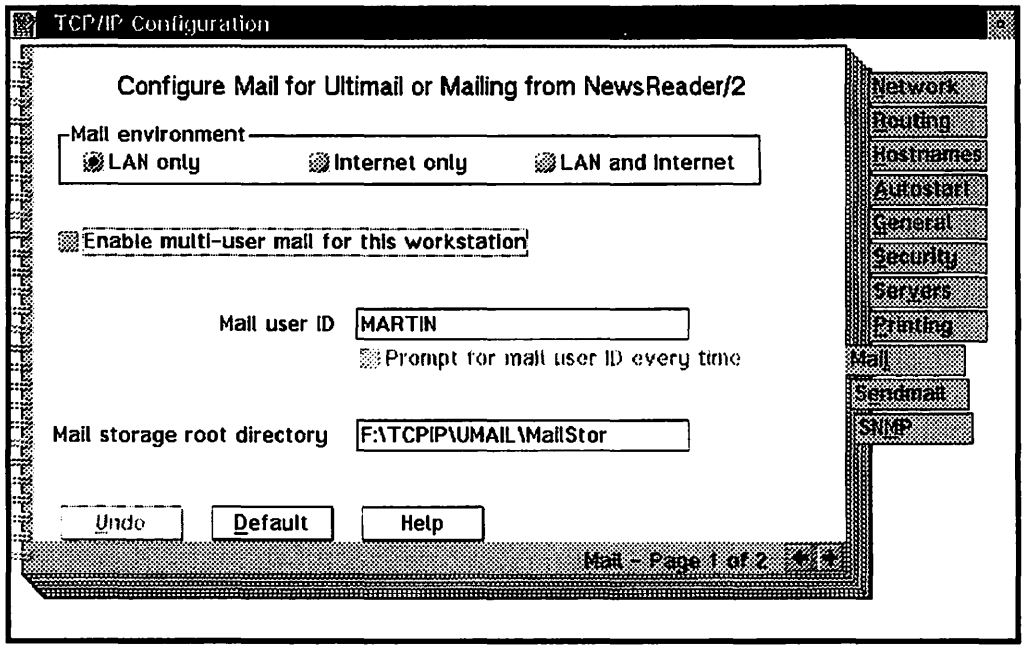


Figure 140. TCP/IP Services Configuration Notebook - Configure Mail for Ultimail or Mailing from NewsReader/2

The following table summarizes the configuration parameters of this page and describes their purposes.

Table 45. TCP/IP Services Configuration Notebook - Mail Page 1	
Configuration Item	**Configuration Data**
LAN only	Select this option, if you will send and receive e-mail over LAN connections only.
Internet only	Select this option, if you will send and receive e-mail over the Internet Connection only.
LAN and Internet	Select this option, if you will send and receive e-mail over LAN connections as well as through your Internet service provider(s).
Enable multi-user mail for this workstation	Check here, if you want to allow several persons to handle their e-mail on your system. **Note:** This is *not* a mailbox which collects and stores e-mail centrally on behalf of other systems that just happen to be inactive when mail arrives for them.
Mail user ID	A name that you wish to use as a mail user ID. The default will be the hostname of your system. The mail user ID will be transformed into: <userID>@<hostname>.<domainname>
Prompt for mail user ID every time	When you have selected the multi-user mail option, you can enable UltiMail to prompt each user for a user ID by checking this box.
Mail storage root directory	The first level directory, under which incoming and undelivered outgoing mail will be stored.

Figure 141 on page 191 shows the Configure POP for Ultimail or Mailing from NewsReader/2 page of the configuration notebook. On this page, you can configure the environment for Multimedia mail when using TCP/IP Services.

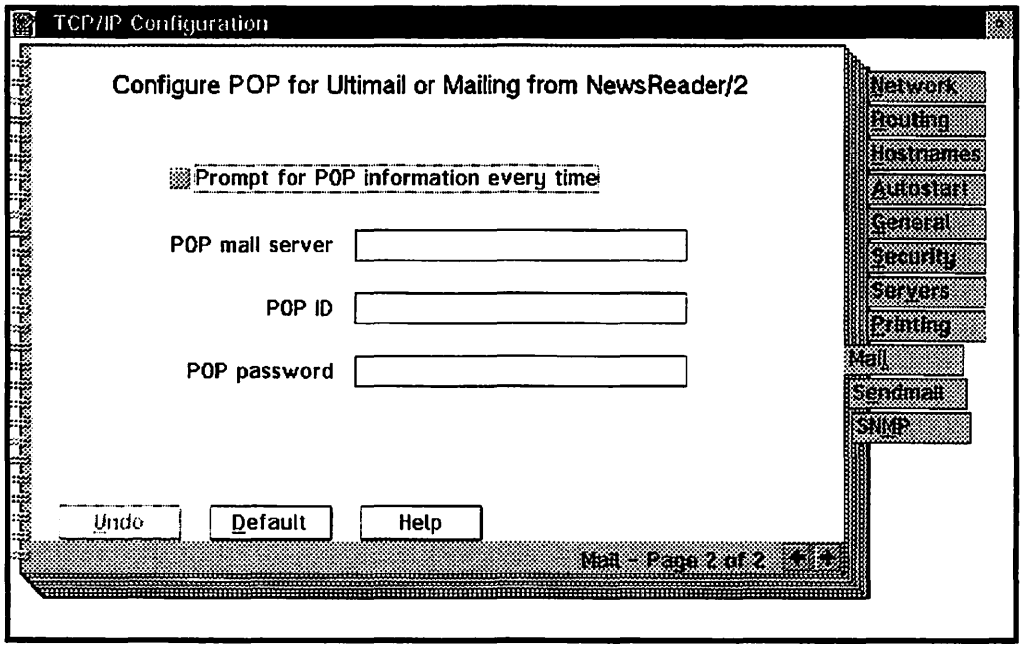


Figure 141. TCP/IP Services Configuration Notebook - Configure POP for Ultimail or Mailing from NewsReader/2

The following table summarizes the configuration parameters of this page and describes their purposes.

Table 46. TCP/IP Services Configuration Notebook - Mail Page 2

Configuration Item	Configuration Data
Prompt for POP information every time	Check this option, if you have enabled multi-user mail, or if you are using multiple POP servers.
POP mail server	The hostname of your mail server on the LAN.
POP ID	Your user ID at the mail server.
POP password	Your password at the mail server.

Configure Sendmail

Figure 142 on page 192 shows the first Configure Sendmail Parameters page of the configuration notebook. On this page, you can configure the electronic mail program of TCP/IP Services.

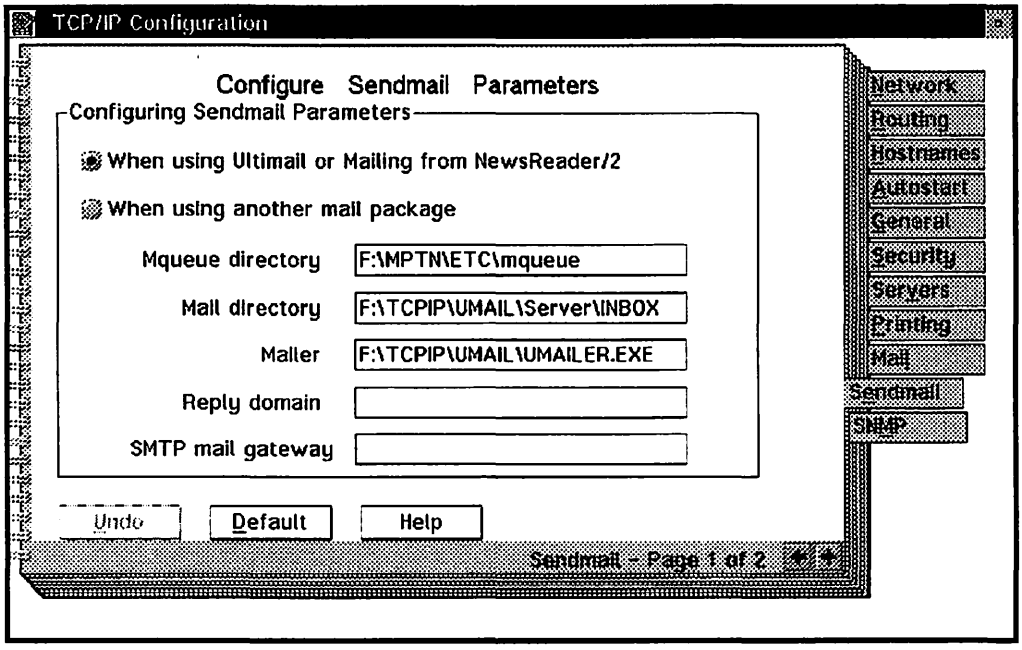


Figure 142. TCP/IP Services Configuration Notebook - Configure Sendmail Parameters

The following table summarizes the configuration parameters of this page and describes their purposes.

Table 47. TCP/IP Services Configuration Notebook - Sendmail Page 1

Configuration Item	Configuration Data
When using Ultimail or Mailing from NewsReader/2	Select this option, if you are using Ultimail or mailing from NewsReader/2
When using another mail package	Select this option, of you will not use Ultimail or mailing from NewsReader/2.
Mqueue directory	Directory to store undelivered outgoing mail.
Mail directory	Directory to store incoming mail.
Mailer	Name of the mail program that you want to use for e-mail.
Reply domain	The name of the domain to which your mail server belongs.
SMTP mail gateway	The hostname of your mail server.

Figure 143 on page 193 shows the second Configure Sendmail Parameters page of the configuration notebook. On this page, you can configure the electronic mail program of TCP/IP Services.

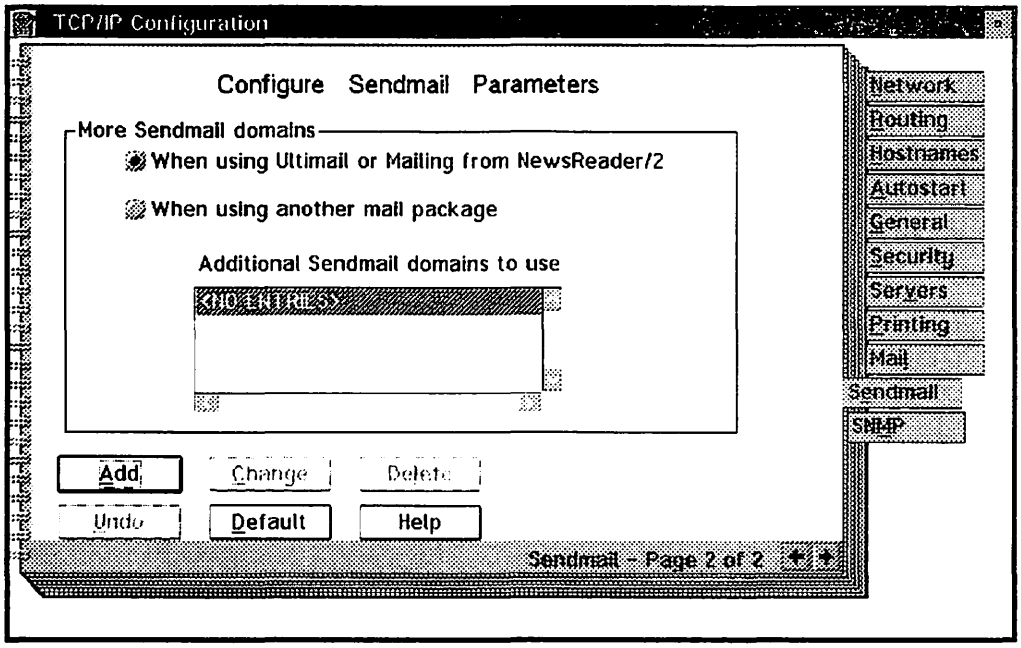


Figure 143. TCP/IP Services Configuration Notebook - Configure Sendmail Parameters

The following table summarizes the configuration parameters of this page and describes their purposes.

Table 48. TCP/IP Services Configuration Notebook - Sendmail Page 2

Configuration Item	Configuration Data
When using Ultimail or Mailing from NewsReader/2	Select this option, if you are using Ultimail or mailing from NewsReader/2.
When using another mail package	Select this option, if you will not use Ultimail or mailing from NewsReader/2.
Additional Sendmail domains to use	Specify up to three additional domains that you can reach over the LAN. This will ensure that e-mail can be delivered properly when you are using a dial-up connection in addition to your LAN connection.

Configure SNMP

Figure 144 on page 194 shows the first Configure SNMP page of the configuration notebook. On this page, you can configure parameters for systems management when using TCP/IP Services.

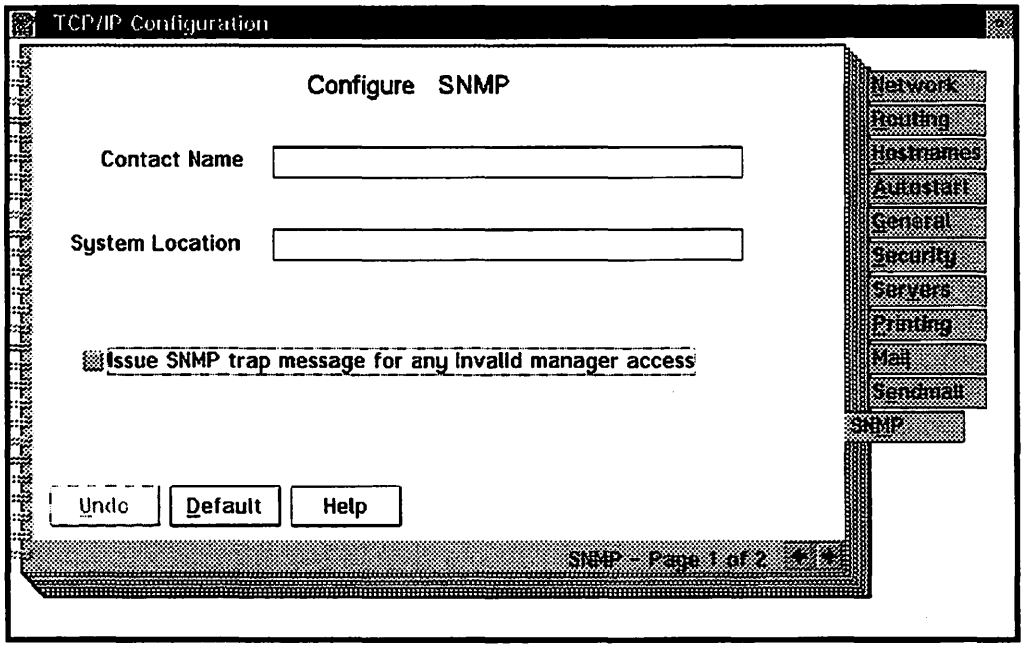


Figure 144. TCP/IP Services Configuration Notebook - Configure SNMP Page 1

The following table summarizes the configuration parameters of this page and describes their purposes.

Table 49. TCP/IP Services Configuration Notebook - SNMP Page 1

Configuration Item	Configuration Data
Contact name	The name of the contact person for this system, and how to reach him or her.
System location	The physical location of this system.
Issue SNMP trap message for any invalid manager access	Check this box, if you want to send SNMP traps whenever an invalid attempt is made by an SNMP manager to access your system.

Figure 145 on page 195 shows the second Configure SNMP page of the configuration notebook. On this page, you can configure parameters for systems management when using TCP/IP Services.

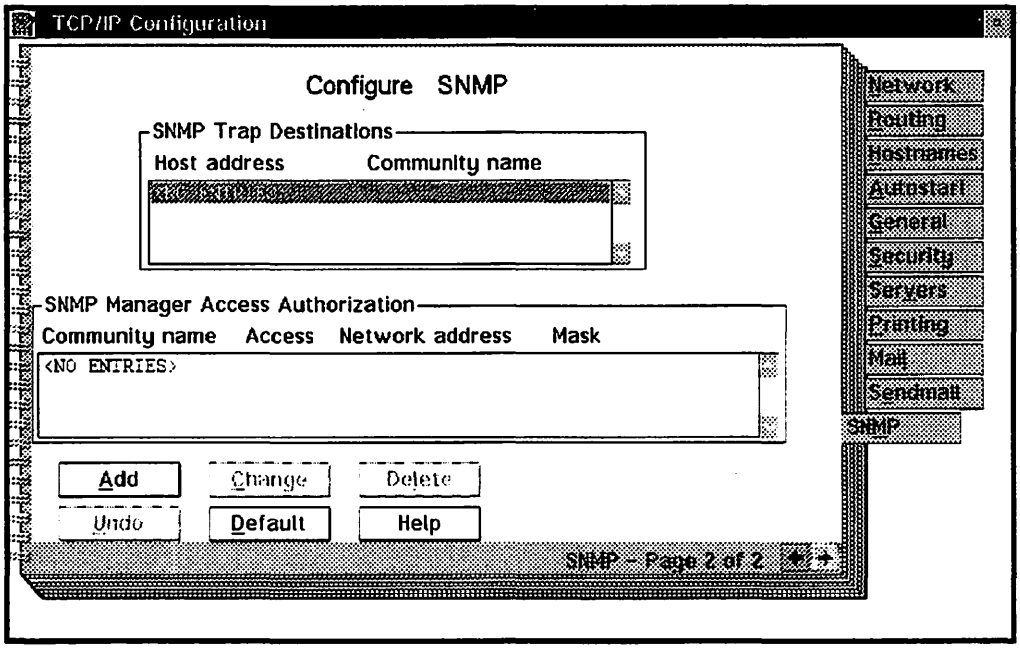


Figure 145. TCP/IP Services Configuration Notebook - Configure SNMP Page 2

Use the SNMP Trap Destinations menu to designate which SNMP managers are to receive SNMP alert messages (traps) from your OS/2 Warp Server system. The list shows the contents of an existing SNMPTRP.LST file. You can add, change and delete entries from this list, as you require. Figure 146 shows the SNMP Manager Access Authorization menu of the second SNMP page.

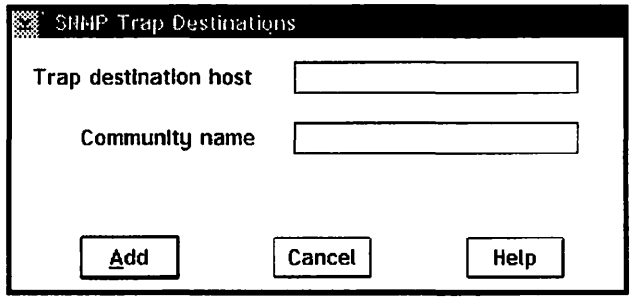


Figure 146. TCP/IP Services SNMP Page 2 - SNMP Trap Destinations

The following table summarizes the configuration parameters of this menu and describes their purposes.

Table 50. TCP/IP Services SNMP Page 2 - SNMP Trap Destinations

Configuration Item	Configuration Data
Trap destination host	The IP address of a host that is to receive SNMP traps from your system.
Community name	A character string that serves as a password in SNMP operations.

Use the SNMP Manager Access Authorization menu to configure SNMP access control. The list shows the contents of an existing PW.SRC file. You can add, change and delete entries from this list, as you require. Figure 147 on page 196

shows the SNMP Manager Access Authorization menu of the second SNMP page.

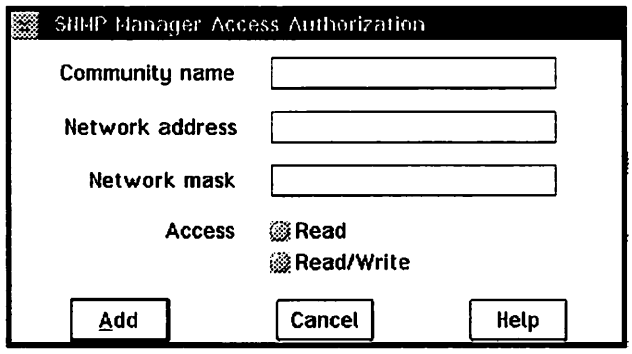


Figure 147. TCP/IP Services SNMP Page 2 - SNMP Manager Access Authorization

The following table summarizes the configuration parameters of this menu and describes their purposes.

Table 51. TCP/IP Services SNMP Page 2 - SNMP Manager Access Authorization

Configuration Item	Configuration Data
Community name	A character string that serves as a password in SNMP operations.
Network address	An IP base network address for which the given password shall be valid.
Network mask	The subnet mask for the above IP address.
Access	Specify the way in which SNMP managers can access information on your system.

When you have finished the configuration of TCP/IP Services, close the Configuration Notebook by double clicking in the top right-hand corner of the window. Select **Save** to close the notebook, and save all changes to your hard disk.

Files Containing TCP/IP Configuration Data

TCP/IP Services configuration data is kept in several files on the drive where OS/2 Warp Server has been installed. Most of those files can be found in the \MPTN\ETC subdirectory of the OS/2 boot drive. TCP/IP Services will also place an icon in the Startup folder to execute the \TCPIP\BIN\TCPSTART.CMD command file at system start. This file will start all TCP/IP client and server applications that you have selected to be autostarted.

The following is a list of the files that are created, updated or modified by the TCP/IP Configuration Notebook:

Table 52 (Page 1 of 2). Files Modified by the TCP/IP Services Configuration Notebook

CONFIG.SYS (OS/2)	TCPOS2.INI (Base)
EXPLORE.INI (WebExplorer)	SETUP.CMD (Base)
NR2.INI (NR2)	GOPHER.INI (Gopher)
TCPSTART.CMD (Base)	SENDMAIL.CF (SENDMAIL)

Table 52 (Page 2 of 2). Files Modified by the TCP/IP Services Configuration Notebook	
RHOSTS (RSH)	RESOLV2 (Base)
SENDMAIL.UML (Ultimail)	INETD.LST (INETD)
HOSTS (Base)	SNMP.INI (SNMPD)
TRUSERS (FTP)	

5.4 A Short Introduction to Dynamic IP

This section describes the purpose of Dynamic IP and the benefits that can be derived from it. We will also introduce the Dynamic IP components and give an overview of the design concepts as well as the actual product implementations as they are contained in OS/2 Warp Server.

Note: We have deliberately included a rather detailed description of DHCP and DDNS because these functions may be new to the majority of TCP/IP users and system administrators. We also wanted to provide at least some basic information on what you may see in configuration files, log files and traces when you need to troubleshoot the OS/2 DHCP and DDNS servers.

To add a new workstation to an IP network, several parameters and a variety of information is required to configure the TCP/IP software. Network components, such as a domain name server, are also required. A new TCP/IP host would normally require the following information:

1. IP address
2. IP subnet mask
3. Default router address
4. Local hostname
5. Domain name
6. Name server address

Additional parameters, such as other server addresses, time zones or protocol specific configurations, may be necessary in some cases.

Keeping track of that information in a large TCP/IP network may not always be an easy task for network administrators, especially if users or machines, or both, change their location frequently. IP address lists and domain name server databases have to be updated manually in order to keep track of any changes in the network.

From a user's point of view, a system administrator would have to be called to provide the necessary information in order to install a TCP/IP system. If the user moves to another location, this information must not be taken; the user will have to be assigned at least a new IP address if not a new hostname as well. Smart users may, thus, cause potential disorder in a TCP/IP network.

Even if workstations will be automatically installed using software distribution techniques, the TCP/IP configuration parameters have to be pre-assigned per distribution client.

The Bootstrap Protocol (BootP), as described in RFCs 951 and 1497, was introduced to the TCP/IP community in 1985 to provide automatic assignment of some TCP/IP configuration parameters to a new TCP/IP host. A table has to be

maintained at BootP servers to enter information specific to any client that has been planned for installation. Typically, clients are identified by their LAN adapter's hardware address which has to be known to the system administrator in charge of a BootP server before he can prepare a new client entry in the database. Even though some manufacturers nowadays put the adapter hardware address on a label on the backplane of their LAN adapters, this ends up being a tedious process if many hosts have to be installed in a short period of time.

Objectives and Customer Benefits of Dynamic IP

To overcome the problems of having to manually update any centrally maintained information files and of having a user manually configure a TCP/IP workstation, the Dynamic Host Configuration Protocol (DHCP) has been designed and is described in an IETF DHC working group Internet draft and in RFCs 1533, 1534, 1541, and 1542. A DHCP server need not be pre-configured with a workstation's LAN address in order to submit the necessary TCP/IP configuration to it.

With DHCP in place, the assignment of IP addresses has become a lot easier. One problem still persists - how would a domain name server learn about those dynamically assigned IP addresses and hostnames so it can update its database accordingly? This can be solved by the Dynamic Domain Name Services (DDNS) as proposed by an IETF DNSIND working group Internet draft.

Having DHCP and DDNS available gives system administrators the advantage of a high degree of flexibility and automation, and users do not have to worry about TCP/IP configuration parameters anymore. Persons in charge of information technology investment budgets may also prefer to spend their money on open standards which will give them the assurance that products from different vendors will coexist in their TCP/IP networks.

IBM is actively participating in the designs and implementations of DHCP and DDNS, and it has coined the term *Dynamic IP*. To summarize, the objectives of Dynamic IP and its benefits to TCP/IP system administrators and users are as follows:

- Provides automatic IP network access and host configuration
- Simplifies IP network administration
- Leverages existing IP network products and infrastructure
- Employs only open standards
- Allows customers to administer site-specific host environments
- Enables customized, location-sensitive parameter setups

The following sections will discuss the DHCP and DDNS protocols in more detail and give examples of their implementations.

Dynamic IP Components: Table 53 on page 199 gives a brief description of the four types of network components which comprise Dynamic IP.

Table 53. DHCP Server Configuration	
System Component	**Description**
Dynamic IP Hosts	Dynamic IP hosts contain DHCP client software and Dynamic DNS client software. Together, they discover and cooperate with their DHCP and Dynamic DNS server counterparts in the network to automatically configure the hosts for network participation.
DHCP Servers	DHCP servers provide the addresses and configuration information to DHCP and BootP clients on the network. DHCP servers contain information about the network configuration and about host operational parameters, as specified by the network administrator.
DDNS Servers	Dynamic DNS servers are a superset of today's static DNS BIND servers. The dynamic enhancements enable client hosts to dynamically register their name and address mappings in the DNS tables directly, rather than having an administrator manually perform the updates.
BootP Relay Agents (or BootP Helpers)	BootP relay agents may be used in IP router products to pass information between DHCP clients and servers. BootP relays eliminate the need for having a DHCP server on each subnet to service broadcast requests from DHCP clients.

5.5 Dynamic Host Configuration Protocol (DHCP)

Dynamic Host Configuration Protocol (DHCP) provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BootP), adding the capability of automatic allocation of reusable network addresses and additional configuration options. DHCP captures the behavior of BootP relay agents, and DHCP participants can interoperate with BootP participants.

In contrast to BootP, DHCP offers the possibility to assign an IP address to a client for a limited amount of time, and it also offers a way to supply all required configuration parameters for a client. This is not possible with BootP.

The following paragraphs provide a brief outline of the DHCP client and server protocol. For a more detailed explanation, please see the latest version of the IETF DHC Internet draft which is available online on the Worldwide Web at the following URL:

`http://www.ietf.cnri.reston.va.us/ids.by.wg/dhc.html`

DHCP Initialization and Acquisition Process

This section describes the initial interaction between DHCP clients and servers. If a client uses multiple IP interfaces, each of them must be configured by DHCP separately. The following steps shows how a DHCP client is initialized:

1. When a client host is started and the DHCP client is initialized for the first time, the client will broadcast a DHCPDISCOVER message on the network, sending it to UDP port 67, the BootP server's well-known port. The client itself uses UDP port 68, the BootP client's well-known port. Using these

ports, and also using the BootP message format as explained later, will ensure that a DHCP server can service both DHCP and BootP clients. The client is then said to be in INIT state.

2. If a DHCP server is not located on the same IP subnet as the client, an intermediate IP router may act as a BootP relay agent and forward any DHCP and BootP messages to a DHCP server (or to another intermediate IP router that has the same capability). In this case, the router will insert its own IP address from the subnet on which the client is located so any DHCP servers can decide if they have an appropriate IP address to offer for that particular client request.

3. To be able to send initial DHCP broadcast messages, a DHCP client configures its IP interface(s) with an address of 0.0.0.0 and sends the broadcast to IP address 255.255.255.255.

   In order to receive DHCP reply messages at a client whose IP stack has not been configured, the TCP/IP implementation at the client must be able to pass on IP packets that are sent to the client's hardware address to the IP layer in that system. Otherwise, DHCP servers (and eventually involved BootP relay agents) must use broadcast frames to submit their information to the client. A client will indicate its ability to receive unicast datagrams rather than broadcast by not setting the broadcast bit in the *flags field* of a DHCP message.

4. DHCP servers that receive DHCPDISCOVER messages will respond with a DHCPOFFER message if they have any IP addresses available. If no addresses are available at a server, it will not respond at all. A DHCP server will include an available IP address and other options in that message. Servers may also check if an offered IP address is not already in use. They can do so using an ICMP echo request (PING). Servers may also temporarily reserve any offered IP addresses so they will not be offered to several DHCP clients at the same time.

5. A client may receive several DHCPOFFER messages from a number of DHCP servers, and it is up to the implementation of the client software to decide which server's offer the client should finally decide to accept. If a server has been selected, the client broadcasts a DHCPREQUEST message to that server whose IP address is contained in the *server identifier* option from the previous DHCPOFFER message.

6. The server that receives a DHCPREQUEST message from a client will finally commit the requested IP address and optimal parameters to its configuration and acknowledge that to the client by sending a DHCPACK message. If that server at that time cannot, for whatever reason, supply any of the requested configuration parameters, it will send a DHCPNACK message instead. The client will then have to repeat the whole acquisition process, starting with a DHCPDISCOVER message.

7. After receiving DHCPACK, the client should also check if the offered IP address is not already in use. This can be done using ARP rather than PING since, at that time, the client has no IP host address it can use. If the offered address is already in use, the client responds with a DHCPDECLINE message to the server; otherwise it will configure its IP interface(s) according to the values obtained from the DHCP server. The client is now fully configured, which is also referred to as the BOUND state.

8. After sending a DHCPDECLINE message, the client must restart the whole acquisition process, starting with a DHCPDISCOVER message. The server, in

this case, must mark that address as not available, and it may notify the administrator with an error message.

9. If a client does not receive any DHCPOFFER messages, it will continue to broadcast DHCPDISCOVER messages at random intervals for a certain period of time before it will notify the user with an error message that it could not obtain any TCP/IP configuration parameters.
10. When a client no longer needs a given TCP/IP configuration, it may inform the server about that using a DHCPRELEASE message. The server will then mark the IP address as available. This message will not be acknowledged by the server.

DHCP Renewing, Rebinding and Rebooting Processes

This section describes the interaction between DHCP servers and clients that have already been configured. If a client uses multiple IP interfaces, each of them must be configured separately by DHCP. The following describes steps for rebinding and rebooting:

1. After a DHCP client has applied the TCP/IP configuration parameters which it has obtained from a DHCP server, it has also received a lease time during which the client is rightfully entitled to use the given configuration. Two timers, T1 and T2, will start to tick down. While T1 will expire before T2, T2 will expire before the end of the assigned lease time. According to the latest IETF Internet draft, T1 defaults to 0.5 times of a lease time, and T2 defaults to 0.875 times of a lease time, but either timer can be set by the server through DHCP options.
2. When timer T1 expires, the client will send a DHCPREQUEST message to the server asking to extend the lease for the given configuration. This state of a client is called the RENEWING state. The server would usually respond with a DHCPACK message indicating the new lease time to which T1 and T2 will then be reset accordingly.
3. If no DHCPACK is received until timer T2 expires, the client enters the REBINDING state. It now has to broadcast a DHCPREQUEST message to extend its lease. This request can be confirmed by a DHCPACK message from any DHCP server on the network.
4. If the client does not receive a DHCPACK message after its lease has expired, it has to stop using its current TCP/IP configuration and may start over from the INIT state as described earlier.
5. If a client has been configured before and is rebooted, it may want to use the previous configuration values which may have been stored in a file on the client's hard disk. In that case, the client would broadcast a DHCPREQUEST message containing the desired parameters in the appropriate option fields. DHCP servers will respond with DHCPACK messages if they can supply the requested configuration. If no DHCPACK messages are received by the client, it may wait and then start over from INIT state as described earlier.
6. If a client is using external configuration values (external to DHCP), which it may have obtained though manual configuration, it would assemble a DHCPINFORM message containing its current configuration and any additionally desired parameters. If the client knows a DHCP server's IP address, it will send this message to that address; otherwise it will broadcast the message. A server will respond to that request using a DHCPACK message which only contains the additionally required options for the client.

If the client does not receive any replies, it should notify the user of that problem and continue operation using suitable defaults.

Figure 148 shows the state transition diagram for a DHCP client to illustrate the descriptions from above. Start reading the diagram from the **INIT** box. Broken lines indicate broadcast messages.

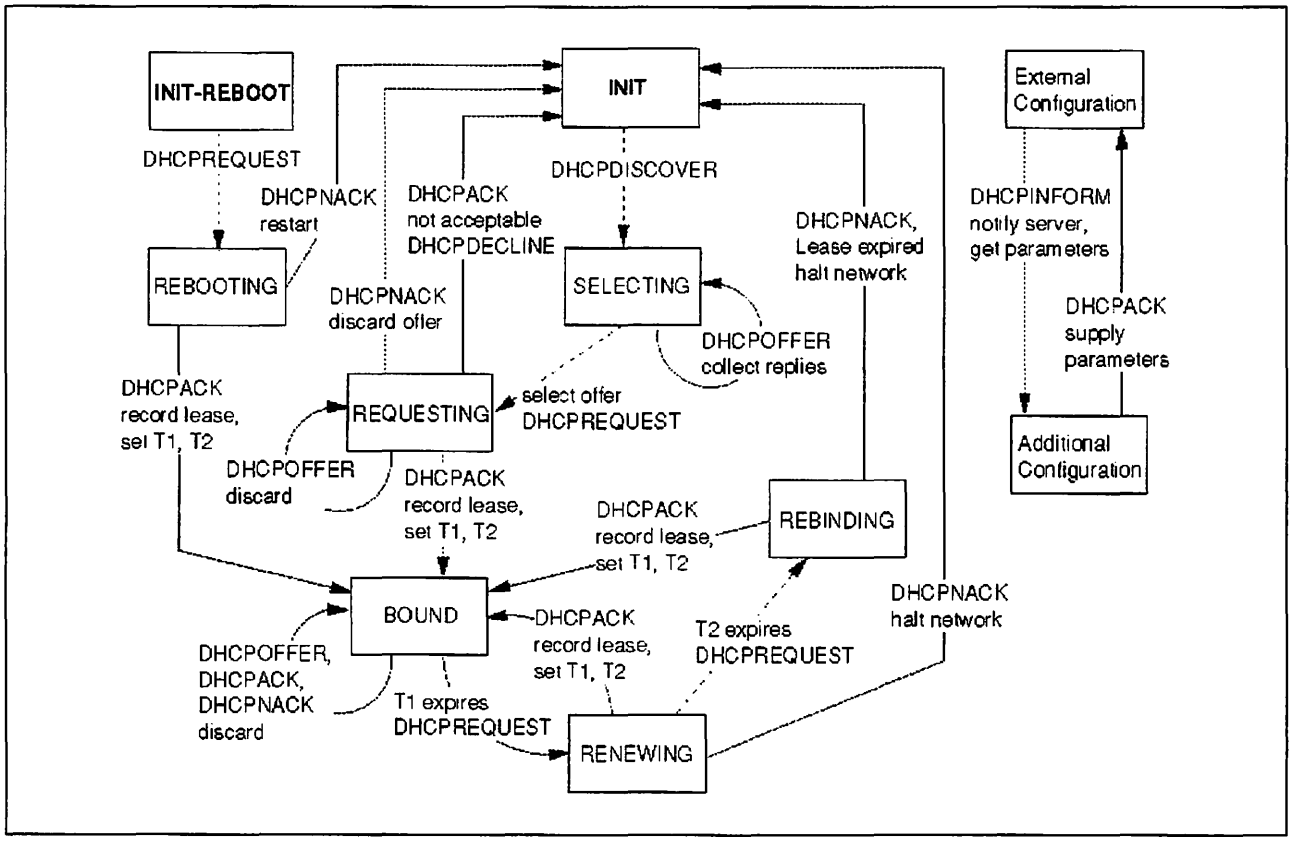


Figure 148. DHCP Client State Transition Diagram

DHCP Message Types and Message Format

This section provides you more detail of the DHCP messages with their format information. The information should help you in case of problem determination. You may skip this section if you feel this is too detail. Table 54 lists the types of messages that can flow between DHCP client and DHCP server systems.

Table 54 (Page 1 of 2). DHCP Message Types

Message	Direction	Use
DHCPDISCOVER	Client to server	Locate available servers
DHCPOFFER	Server to client	Offer available configuration parameters
DHCPREQUEST	Client to server	1. Request offered parameters 2. Confirm correctness of previously allocated address 3. Extend lease on a particular address
DHCPACK	Server to client	Commit requested address

Table 54 (Page 2 of 2). DHCP Message Types		
Message	**Direction**	**Use**
DHCPNACK	Server to client	1. Requested address cannot be supplied 2. Requested address is invalid because client has moved to a different IP subnet 3. Lease for an address has expired
DHCPDECLINE	Client to server	Address is already in use
DHCPRELEASE	Client to server	Address is no longer needed; current lease will be cancelled
DHCPINFORM	Client to server	Asking for additional parameters only; address already configured

DHCP uses the BootP message format, as defined in RFC 951, which is shown in the diagram below:

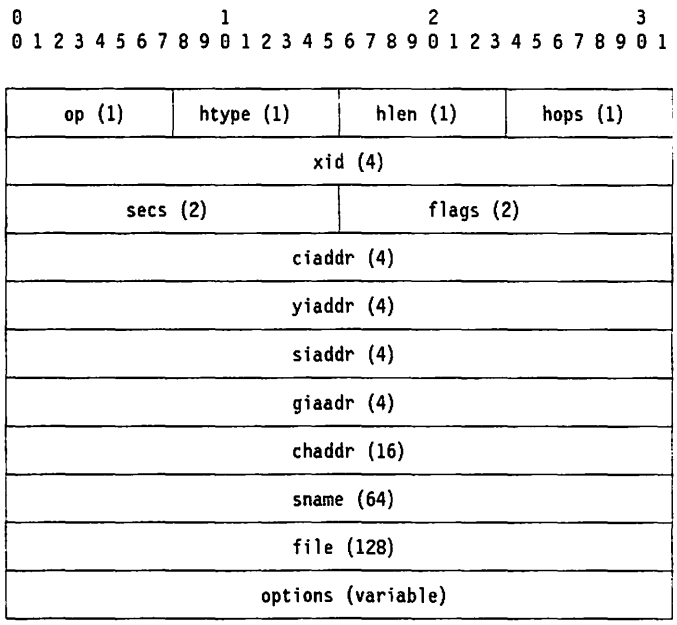


Figure 149. DHCP Message Format

Table 55 explains the fields used within a DHCP message.

Table 55 (Page 1 of 2). DHCP Message Fields		
Field	**Number of Bytes**	**Description**
op	1	Message operation code; will be: 1 for BOOTREQUEST in messages sent from a client to a DHCP server. 2 for BOOTREPLY in messages sent from a DHCP server to clients.
htype	1	Hardware address type as used by ARP, for instance 6 for token-ring.
hlen	1	Hardware address length, for instance 6 for token-ring.

Table 55 (Page 2 of 2). DHCP Message Fields		
Field	**Number of Bytes**	**Description**
hops	1	Set to 0 by clients. This field may optionally be used by BootP relay agents if client and server are not on the same IP subnet.
xid	4	Transaction ID; a random number chosen by the client. This field is used by clients and servers to associate messages and responses between a client and a server.
secs	2	This field is filled in by the client. It represents the number of seconds that have elapsed since the client began the address acquisition or the lease renewal process.
flags	2	Only broadcast flag used to determine if client is able to accept IP unicast datagrams.
ciaddr	4	Client IP address. Filled in by the client. Set to 0 or client's IP address.
yiaddr	4	Your (client) IP address. Filled in by the DHCP server.
siaddr	4	Server IP address. Returned by the server in DHCPOFFER and DHCPACK messages.
giaddr	4	Gateway IP address. Inserted when a BootP relay agent is being used.
chaddr	16	Client hardware address. Filled in by the client.
sname	64	Server hostname. An optional field containing a null-terminated string.
file	128	BootP file name. Used when a DHCP server is employed to provide operating system startup files for BootP clients.
options	variable	Optional parameters. See explanations below.

Though the *options* field has a variable length, DHCP clients must be able to receive messages with an options field of a length of 312 bytes. This implies that a client must be configured to receive a message of 576 bytes, which is the minimum IP datagram size that a client must be prepared to accept anyway.

A DHCP server may also use the *sname* and/or *file* fields to transmit additional DHCP options. It will then inform a client about this by coding a special option. The client will then evaluate those fields after it has gone through the regular options.

DHCP options are grouped by categories, as shown in Table 56.

Table 56 (Page 1 of 2). DHCP Options		
Group	**Range**	**Description**
Base options	1-18	BootP vendor extensions as defined in RFC 1497.
IP layer parameters per host	19-25	Options that affect the operation of the IP layer on a per-host basis.

Table 56 (Page 2 of 2). DHCP Options		
Group	**Range**	**Description**
IP layer parameters per interface	26-33	Options that affect the operation of the IP layer on a per-interface basis. Multiple requests should be possible to configure multiple interfaces separately.
Link layer parameters per interface	34-36	Options that affect the operation of the data link layer on a per-interface basis.
TCP parameters	37-39	Options that affect the operation of the TCP layer on a per-interface basis.
Application and service parameters	40-49	Options to configure miscellaneous applications and services.
DHCP extensions	50-61, 77	Options that are specific to DHCP.
Application and service extensions	64-76	Additional options to configure miscellaneous applications and services.
User-defined extensions	78-127	Reserved for future use.
Site-specific options	129-253	Options used for experimental usage or to provide site-specific configuration parameters.

Options 128 and 254 are reserved. Additional options may be registered with the Internet Assigned Numbers Authority (IANA), by sending e-mail to iana@isi.edu. The first four bytes in the options field should always be hex 63.82.53.63, the magic cookie as mentioned in RFC 951.

For a detailed description of DHCP options, please refer to RFC 1533 available online on the Worldwide Web at the following URL:

`http://ds.internic.net/ds/rfc-index.html`

5.6 Configuring an OS/2 DHCP Server

Product differentiation and the value of DHCP server products lie in their ease of use and in the flexibility in setting up policies that can be made available to administrators. The IBM OS/2 DHCP server includes a graphical configuration program that facilitates the creation and maintenance of the DHCP server database. The server also gives administrators the following options:

- Flexibility to configure hosts individually, based on a designated class or based on their location in the network.
- Configure site-specific applications on client hosts with information defined centrally at DHCP servers, effectively extending and customizing the Dynamic IP system to serve the needs of the enterprise.
- Use of vendor-specific options to supply specific configuration parameters to clients from different vendors.

There are three ways of supporting clients with the OS/2 DHCP server:

1. Dynamic
2. Automatic
3. Manual

When used dynamically, the DHCP server assigns IP addresses from an address pool for a limited period of time (leased). The client must then periodically renew its lease of an IP address, but this is done automatically without user or administrator intervention.

When used automatically, the DHCP server assigns IP addresses from an address pool for an unlimited period of time (permanent).

When used manually, the DHCP server assigns a specific, pre-defined address to a specific client. This type of IP address assignment can be used to support BootP clients with the DHCP server.

Figure 150 shows the DHCP services folder from which the DHCP server program and the DHCP server configuration program can be started.

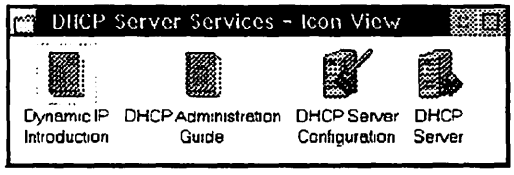


Figure 150. DHCP Services Folder

To start the DHCP server configuration program, double-click on the appropriate icon in the DHCP Server Services folder. The configuration program offers you a graphical interface to administer your DHCP server parameters. Figure 151 shows the DHCP server configuration program.

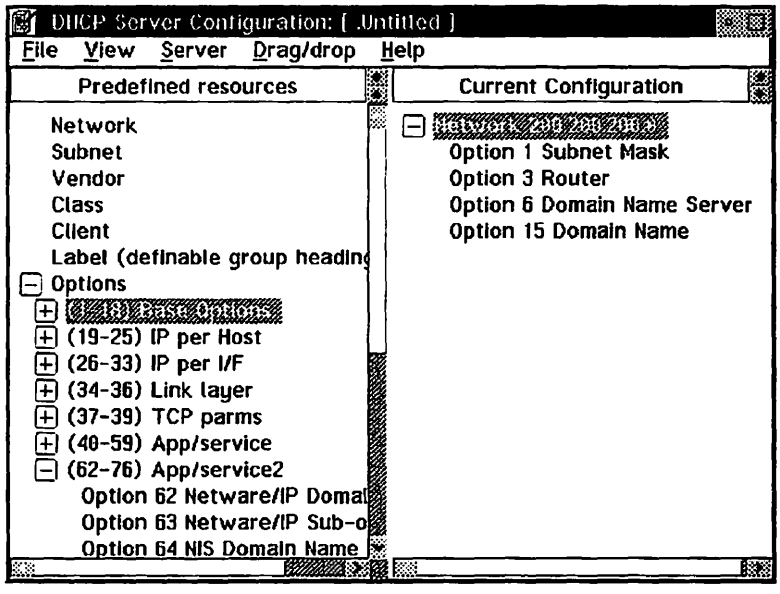


Figure 151. DHCP Server Configuration Program

On the left side of the configuration program, the Predefined resources window is displayed. Items that can have a set of definitions are prefixed with a plus sign (+). Click there to expand any item to reveal parameters located one level below.

On the right side of the configuration program, you see the Current Configuration window. To add items, select the appropriate parameter from the Predefined

Resources window, then click on it with the right mouse button. Using mouse button 2, drag the item from the left side to the right side of the configuration program, then drop it onto the current configuration by releasing the mouse button 2.

To remove an item from the Current Configuration window, simply drag the item to the OS/2 shredder and drop it there.

Once an item has been dragged and dropped to your configuration, you can configure any required values by double-clicking on the item.

Note: You can only double-click on an item in the Current Configuration window, not in the Predefined resources window.

The following table summarizes the configuration parameters of the Predefined resources window and describes their purposes.

Table 57. DHCP Server Configuration - Predefined Resources Window

Configuration Item	Configuration Data
Network	The network statement specifies one network that is administered by a server. A network starts at a base IP network address and may consist of one or more subnets or a range of IP addresses. There may be multiple network statements indicating that a server will control more than one network.
Subnet	The subnet statement specifies one subnet under a network statement. A subnet starts at a base IP subnet address and may include all IP addresses of that subnet or only a specified range of addresses. There may be multiple subnet statements under a network statement.
Vendor	A specific set of configuration parameters to be used with a client from a certain vendor.
Class	A specification for a set of clients. May include a range of IP addresses and a set of options. DHCP clients which request this class will be given the specified options and valid addresses. This configuration can be used to group clients according to business organization.
Client	A specific definition for a client. May be used to serve clients individually, to exclude clients from participating in DHCP, or to serve BootP client requests.
Label	A comment that will be inserted in the configuration file to make it more readable.
Options	Any of the DHCP options and the values that will be served to DHCP and BootP clients, as appropriate.

Figure 152 on page 208 shows an example of a DHCP server network configuration.

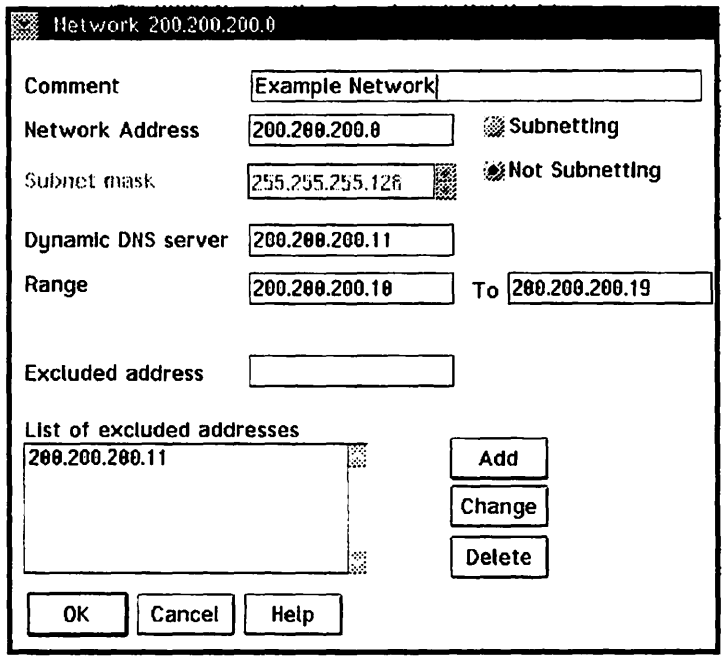


Figure 152. DHCP Server Configuration Program - Network Menu

The following table summarizes the server configuration parameters and describes their purposes.

Table 58. DHCP Server Configuration - Network Menu

Configuration Item	Configuration Data
Comment	Specify a descriptive comment for this network.
Network Address	Enter the base IP address for this network. You should always enter a base IP address here.
Subnet mask	If you clicked on the **Subnetting** button, enter the subnet mask for this network here. The DHCP server will then use all possible IP host addresses for the given network and subnet mask combination. You cannot specify a subnet mask if you clicked on the **Not Subnetting** button. In that case, you have to specify a range of IP addresses to be used by the DHCP server. **Note:** When you use subnetting, you cannot specify a DDNS server and IP addresses to be excluded on the network menu. Those parameters must be configured on the respective subnet menus.
Dynamic DNS server	Enter the IP address of a DDNS server that will be updated by this DHCP server with inverse name resolution information.
Range	If you clicked on the **Not Subnetting** button, specify the range of IP addresses, within this network, to be used by the DHCP server. The DHCP server will then use only IP host addresses that are within the specified range. You cannot specify a range if you clicked on the **Subnetting** button. In that case, you have to specify a subnet mask for this network.
Excluded address	Specify any IP addresses that you want to exclude from the specified subnet or range. Typically, this will be addresses of routers and servers, such as primary DDNS servers. The DHCP server will reserve those addresses and will not lease them to clients.

You can use the Subnet, Vendor, Class, Client, Label, and Options menus in a similar way. To use, for instance, a subnet specification, simply drag that item from the Predefined resources window to the Current configuration window and drop it onto the Network item. This process will create a tree of configuration items.

The scope of an option covers the configuration item where it is specified, for instance a network, and all items below that. Options that are specified outside any item have a global scope.

Apart from the Predefined resources window, there is a User-defined resources window from which to drag items to a configuration. For either side of the configuration program, there is a Scratch pad window for testing. The User-defined resources window and the Scratch pads can be accessed by clicking on the up or down arrows in the windows on top of either side.

To remove an item from the Current Configuration window, simply drag the item to the OS/2 shredder and drop it there.

When you have finished the DHCP server configuration, you can save the parameters to a file using the Save option from the File pull-down menu on the menu bar. By default, a DHCPSD.CFG file will be used by the DHCP server. This file will be searched in the directory where the ETC environment variable points to, normally the \MPTN\ETC subdirectory of the OS/2 boot drive.

The following example shows a DHCP server configuration file that has been created using the configuration program.

```
numLogFiles          2
logFileSize          50
logFileName          dhcpsd.log
leaseTimeDefault     1 hours
leaseExpireInterval  50 minutes
supportBOOTP  no
supportUnlistedClients  yes
logItem      SYSERR
logItem      OBJERR
logItem      PROTERR
logItem      WARNING
logItem      EVENT
logItem      ACTION
logItem      INFO
logItem      ACNTING
logItem      TRACE
#.indent 12

updateDNS "nsupdate -f -r%s -s"d;ptr;*;a;ptr;%s;s;%s;0;q""

network      200.200.200.0  200.200.200.10-200.200.200.19    #.name Example Network
{
    #.ddns 200.200.200.11
    client 0 0 200.200.200.11    #.exclu
    option 1       255.255.255.0    #.name 1 Subnet Mask
    option 3       200.200.200.1    #.name 3 Router
    option 6       200.200.200.11    #.name 6 Domain Name Server
    option 15       test.itsc.austin.ibm.com    #.name 15 Domain Name
}
```

In the example above, the DHCP server controls IP addresses in the range from 200.200.200.10 to 200.200.200.19. It will send updates to the dynamic DNS server 200.200.200.11, and it will therefore exclude this address from the list of addresses available to DHCP clients. Furthermore, DHCP options 1, 3, 6, and 15 will be supplied to DHCP clients. In this example, BootP clients will not be supported by the DHCP server.

To start the OS/2 DHCP server, double-click on the appropriate icon in the DHCP Services folder. Likewise, you can start the server by entering the following command on an OS/2 command prompt:

```
DHCPSD
```

Figure 153 shows the OS/2 DHCP server program.

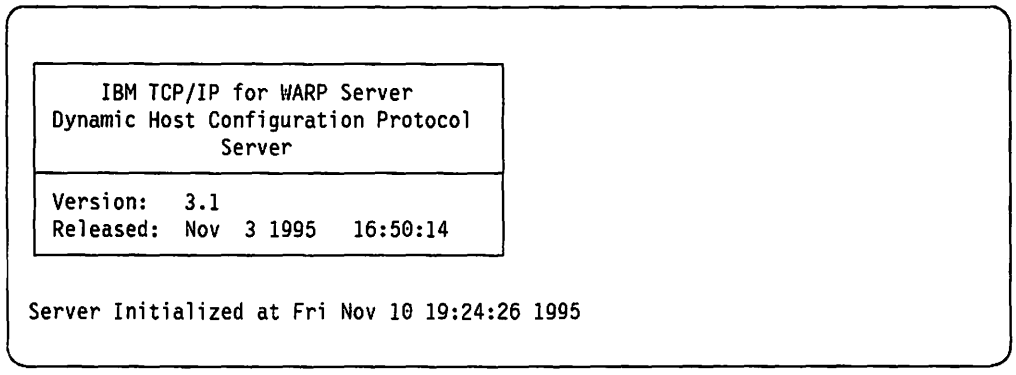

IBM TCP/IP for WARP Server
Dynamic Host Configuration Protocol
Server
Version: 3.1
Released: Nov 3 1995 16:50:14
Server Initialized at Fri Nov 10 19:24:26 1995

Figure 153. OS/2 DHCP Server Program

The OS/2 DHCP server can be configured to log any activities and client requests, which is a very helpful option for problem determination. To activate logging, check the options you want to log from the Server pull-down menu in the configuration program which is shown in Figure 154:

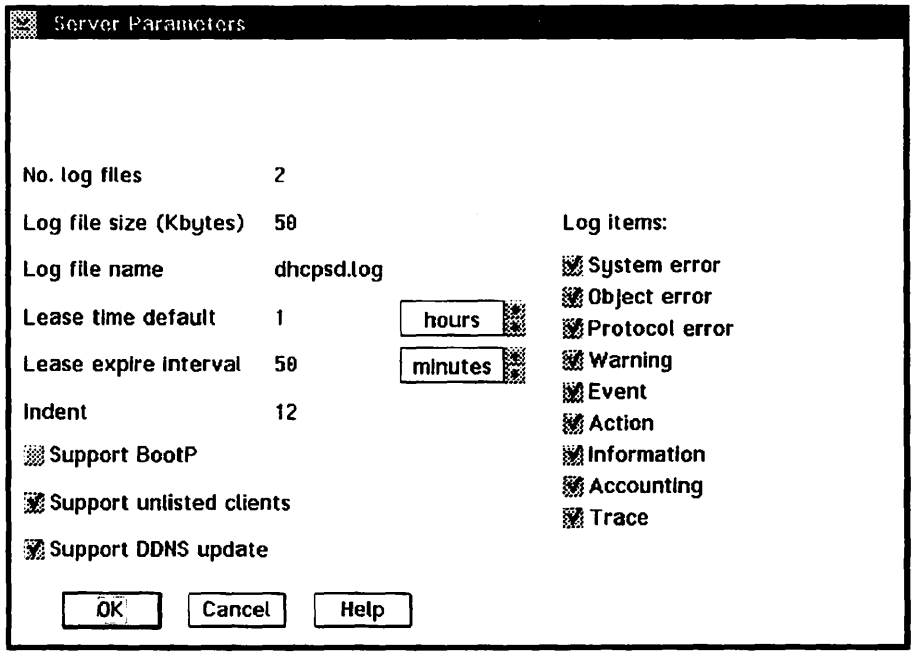


Figure 154. DHCP Server Parameters

The following table summarizes the server configuration parameters and describes their purposes.

Table 59. DHCP Server Configuration - Server Parameters	
Configuration Item	**Configuration Data**
No. log files	Specify how many log files the DHCP server should maintain. The server will gradually fill up the log files and then continue by overwriting the oldest file.
Log file size (Kbytes)	Specify the maximum file size of any log file.
Log file name	Specify the name of the current log file. Completed log files will use the name with consecutive numbers as extensions.
Lease time default	Specify the default lease time for IP addresses.
Lease expire interval	Specify the time interval for the DHCP server to check if leases have expired or are still valid.
Indent	Specify the number in pixels that the DHCP server configuration program should use to indent items in the configuration tree.
Log items:	Click on the type of information you want the server to write to the log file(s).
Support BootP	Click here, if you want to support BootP clients with this DHCP server.
Support unlisted clients	Click here, if you want to support DHCP clients in a dynamic way without having to configure specific information per client.
Support DDNS update	Click here, if you want the DHCP server to update a DDNS server with inverse hostname resolution information. The following statement in the DHCP server configuration file includes the command that is sent to the DDNS server to update PTR records for inverse mapping: `updateDNS "nsupdate -f -r%s -s"d;ptr;*;a;ptr;%s;s;%s;0;q"'` The %s variables will be evaluated by the DHCP server as follows: 1. IP address 2. Fully-qualified hostname 3. Lease time

In order to support DDNS updates, you have to select the respective option on the Server Parameters window. Then click on the **Update DDNS data file** option on the File menu of the DHCP server configuration program. This will create the DHCPSD.DAT file where information about the primary nameserver and the encryption key to be used in DDNS updates are stored. In order to actually enable the DDNS update function, you must merge the information from the DHCPSD.DAT file into the DDNS.DAT file that will be created by the DDNSZONE command when you configure the DDNS server.

The DHCP server will output its logging data to a DHCPSD.LOG file which may look like the following:

```
11/14/95 16:37:43 START:  .....log_initialize: ***************************
11/14/95 16:37:43 START:  .....log_initialize: *     NEW LOG FOLLOWS     *
11/14/95 16:37:43 START:  .....log_initialize: * | | | | | | | | | | | | *
11/14/95 16:37:43 START:  .....log_initialize: * V V V V V V V V V V V V *
11/14/95 16:37:43 START:  .....log_initialize: ***************************
11/14/95 16:37:43 SYSERR: .....log_initialize: Logging ENABLED
11/14/95 16:37:43 OBJERR: .....log_initialize: Logging ENABLED
11/14/95 16:37:43 PROTERR:.....log_initialize: Logging ENABLED
11/14/95 16:37:43 WARNING:.....log_initialize: Logging ENABLED
11/14/95 16:37:43 EVENT:  .....log_initialize: Logging ENABLED
11/14/95 16:37:43 ACTION: .....log_initialize: Logging ENABLED
11/14/95 16:37:43 INFO:   .....log_initialize: Logging ENABLED
```

```
11/14/95 16:37:43 ACNTING:......log_initialize: Logging ENABLED
11/14/95 16:37:43 TRACE:  ......log_initialize: Logging ENABLED
11/14/95 16:37:43 INFO:   ......profile_repository_initialize: end of string not found
11/14/95 16:37:43 INFO:   ........am_initMapper: previous map files not removed; try to accommodate within new conf
11/14/95 16:37:43 TRACE:  ........am_initMapper: previous map 200.200.200.100 : 1-0x0004ac33608b has been adopted
11/14/95 16:37:43 TRACE:  ........am_initMapper: previous map 200.200.200.101 : 6-0x08005aceea89 has been adopted
11/14/95 16:37:43 TRACE:  ........am_initMapper: previous address 200.200.200.102 has been adopted
11/14/95 16:37:43 TRACE:  ........am_initMapper: previous address 200.200.200.103 has been adopted
11/14/95 16:37:43 TRACE:  ........am_initMapper: previous address 200.200.200.104 has been adopted
11/14/95 16:37:43 TRACE:  ........am_initMapper: previous address 200.200.200.105 has been adopted
11/14/95 16:37:43 TRACE:  ........am_initMapper: previous address 200.200.200.106 has been adopted
11/14/95 16:37:43 TRACE:  ........am_initMapper: previous address 200.200.200.107 has been adopted
11/14/95 16:37:43 TRACE:  ........am_initMapper: previous address 200.200.200.108 has been adopted
11/14/95 16:37:43 TRACE:  ........am_initMapper: previous address 200.200.200.109 has been adopted
11/14/95 16:37:43 TRACE:  ........am_initMapper: previous address 200.200.200.110 has been adopted
11/14/95 16:37:43 INFO:   ......getPortNum: dhcps/udp unknown service, assuming port 67
11/14/95 16:39:01 TRACE:  ......SelectFunc: DHCP comm descriptor selected
11/14/95 16:39:01 TRACE:  ....receiveMailbox: size of incoming packet is 548
11/14/95 16:39:01 INFO:   ........primeOptions: Option: 53, length:1
11/14/95 16:39:01 INFO:   ........primeOptions: Option: 50, length:4 value: 1707657416 (0x65c8c8c8)
11/14/95 16:39:01 INFO:   ........primeOptions: Option: 61, length:7
11/14/95 16:39:01 INFO:   ........primeOptions: Option: Parameter Request List, length:6
11/14/95 16:39:01 INFO:   ........primeOptions: Option 1 requested
11/14/95 16:39:01 INFO:   ........primeOptions: Option 3 requested
11/14/95 16:39:01 INFO:   ........primeOptions: Option 6 requested
11/14/95 16:39:01 INFO:   ........primeOptions: Option 15 requested
11/14/95 16:39:01 INFO:   ........primeOptions: Option 28 requested
11/14/95 16:39:01 INFO:   ........primeOptions: Option 33 requested
11/14/95 16:39:01 INFO:   ........primeOptions: Option: 60, length:12
11/14/95 16:39:01 TRACE:  ........identifiableClient: DHCP option Client-identifier specified
11/14/95 16:39:01 TRACE:  ........legibleRequest: DHCP msg type DHCPREQUEST
11/14/95 16:39:01 TRACE:  ......process_bootrequest: request is self-consistent
11/14/95 16:39:01 TRACE:  ..............locateClientRecord: located client 6-0x08005aceea89 in client records
11/14/95 16:39:01 TRACE:  ............am_queryClient: client 6-0x08005aceea89 is known to address mapper, status=4
11/14/95 16:39:01 TRACE:  ..............locateClientRecord: located client 6-0x08005aceea89 in client records
11/14/95 16:39:01 INFO:   ............am_addressClient: client 6-0x08005aceea89 suggested 200.200.200.101 in range
11/14/95 16:39:01 INFO:   ............am_addressClient: client 6-0x08005aceea89 had 200.200.200.101 mapped previou
11/14/95 16:39:01 INFO:   ..........getPortNum: dhcpc/udp unknown service, assuming port 68
11/14/95 16:39:01 INFO:   ......generate_bootreply: generating a DHCPACK reply
11/14/95 16:39:01 INFO:   ......FetchHwType: Found the HW type for interface 0 = 6
11/14/95 16:39:01 TRACE:  ......transmitMailbox: transmitting to (200.200.200.101 #68)
```

In the example above, you can see a DHCP server that has been restarted and now tries to adopt the latest active configuration. The server then receives a DHCPREQUEST message from a DHCP client that has been rebooted. The server checks the requested parameters and responds with a DHCPACK message. In fact, this example matches the DHCP client log file example that is shown on page 232.

When the OS/2 DHCP server has been initialized, it will store the current status of its configuration in the \MPTN\ETC\DHCPS.AR and \MPTN\ETC\DHCPS.CR files. The server will attempt to restore that information again whenever it is restarted.

Configuring Site-Specific Options for OS/2 WARP TCP/IP

To code specific options for an OS/2 WARP TCP/IP client could be done using the vendor option (43), but the syntax of that option is rather complicated. An easier way to supply specific configuration information to OS/2 WARP TCP/IP clients is to use some of the site-specific options, along with application and services options.

On the DHCP client, a program must be run to evaluate those options and set configuration parameters accordingly. In the case of an OS/2 WARP client, the DHCPIBM.CMD file is supplied with Adapter and Protocol Services. It is a REXX command file that evaluates site-specific options and applies the values to the TCP/IP for OS/2 configuration. To activate this mechanism, you must comment out the line for one or more options in the DHCP client configuration file. Please see "OS/2 Dynamic IP Clients" on page 228 for more information on OS/2 DHCP client configuration.

The following table summarizes the configuration parameters for OS/2 WARP TCP/IP clients that can be supplied by site-specific DHCP options:

Table 60. DHCP Server Configuration - Site-Specific Options

Option Number	Description	Modified file
9	IP address of the default LPR server	TCPOS2.INI
71	IP address of the default NewsReader/2 server	TCPOS2.INI
200	Device name of the default LPR printer	TCPOS2.INI
201	IP address of the default Gopher server	TCPOS2.INI
202	URL of the default WWW home page	EXPLORE.INI
203	URL of the default WWW proxy server	EXPLORE.INI
204	IP address of the default WWW news server	EXPLORE.INI
205	IP address of the default SOCKS server, and optionally IP address of the default SOCKS nameserver	TCPOS2.INI
206	NFS client mount string	FSTAB.INI
207	X Window System default font path	PMX.INI
208	The xdmcp command-line for the X Window System display manager	PMX.INI

To configure the site-specific options for OS/2 WARP with the DHCP server configuration program, use option 78 (user-defined option) as many times as you need for the number of options you want to configure. Figure 155 shows the panel for option 78. All you have to do is enter the option number followed by a description in the Comment field; then enter the number again in the Option number field.

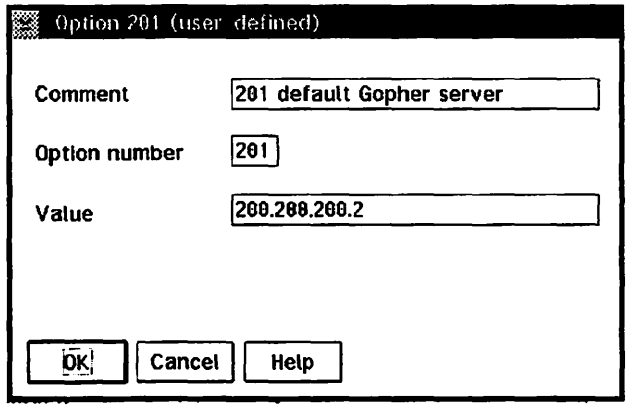


Figure 155. DHCP Server Configuration Program - Site-Specific Options

Notes:

1. When you expand the Options item on the Predefined resources window, you may only see options from 1 to 76. You have to expand the (62-76) App/service2 item, there you will find option 78 at the bottom of the list.
2. The text that is displayed for each site-specific option in the Current configuration window will remain Option 78 as long as you do not save and reload the configuration file.

You can, of course, configure site-specific options manually, if you prefer.

5.7 A Short Introduction to Cryptography

Since the IBM OS/2 DDNS server and client products implement not only dynamic DNS but also DNS security functions, we would like to explain, in very brief terms, the usage of cryptographic processes, courtesy of RSA Data Security, Inc., Redwood City, California.

This section will give you more inside of the RSA security system but this is not a mandately section for you.

Secret Key Cryptography: This method uses a *secret key* to encrypt a message. The same secret key must be used again to decrypt the message. This means that the key must be sent along with the message which exposes it to whoever may be eavesdropping on the conversation. Secret keys are very fast in terms of processing, and it is not easy to break them, even though they are exposed through the communication process.

Public Key Cryptography: This method uses a combination of a modulus and a pair of exponents, called the *public key* and the *private key*. Exponents and modulus must be used together to encrypt or decrypt a message, but only the modulus and the public exponent are communicated since they are important to everyone who wants to send or receive encrypted messages using this method. The private exponent will never be publicly exposed. This ensures that no one else can decrypt messages that have been intended for a specified recipient, nor can anyone else disguise as that recipient in order to intercept a message.

Encryption and Authentication: Encryption means that a message will be scrambled before it can be sent over a communications link. The plain message itself will never be sent in order to ensure privacy. Authentication is used to ensure that a message has indeed originated from the source which is specified in the message, and that the message has not been altered in transit. It additionally serves the purpose of non-repudiation, which means that whoever has digitally signed a message cannot claim later that he or she has not done so. In this case, the plain message itself will be sent since there is no need for privacy. The message will also be used to generate a *digital signature* by using one of the aforementioned cryptographic methods, preferably public keys.

Hash Functions: A hash function is a computation that takes a variable-size input and returns a fixed-size string, which is called the hash value. If the hash function is one-way, that means hard to invert, it is also called a message-digest function, and the result is called a *message digest*. The idea is that a digest represents concisely the longer message or document from which it was computed; one can think of a message digest as a *digital fingerprint* of the larger document.

The RSA Encryption Standard

This standard public key encryption method, along with the MD5 hash function, is used with the IBM DDNS products in OS/2 Warp Server. The principle of the RSA algorithm is as follows:

1. Take two large primes, p and q.
2. Find their product n = p * q; n is called the modulus.
3. Choose a number, e, less than n and relatively prime to (p-1) * (q-1).

4. Find its inverse, d, mod (p-1) * (q-1), which means that e * d = 1 mod (p-1) * (q-1).

e and d are called the public and private exponents, respectively. The public key is the pair (n,e); the private key is d. The factors p and q must be kept secret or destroyed.

An example of RSA privacy (encryption) would be the following:

Suppose Alice wants to send a private message, m, to Bob. Alice creates the ciphertext c by exponentiating:

```
c = m^e mod n
```

where e and n are Bob's public key. To decrypt, Bob also exponentiates:

```
m = c^d mod n
```

and recovers the original message, m; the relationship between e and d ensures that Bob correctly recovers m. Since only Bob knows d, only Bob can decrypt.

An example of RSA authentication would be the following:

Suppose Alice wants to send a signed document, m, to Bob. Alice creates a digital signature s by exponentiating:

```
s = m^d mod n
```

where d and n belong to Alice's key pair. She sends s and m to Bob. To verify the signature, Bob exponentiates and checks that the message, m, is recovered:

```
m = s^e mod n
```

where e and n belong to Alice's public key.

Thus encryption and authentication take place without any sharing of private keys: each person uses only other people's public keys and his or her own private key. Anyone can send an encrypted message or verify a signed message, using only public keys, but only someone in possession of the correct private key can decrypt or sign a message.

To make encryption methods secure, a fairly large modulus should be chosen since it becomes increasingly difficult to break a large number into factors to determine the original primes. RSA uses a minimum length of 512 bits for the modulus, which would convert to a number with approximately 155 digits.

Due to security concerns, public key systems that use a key length of more than 512 bits must not be exported from the US.

For encryption, in reality, RSA is combined with a secret-key crypto system, such as DES, to encrypt a message by means of an RSA *digital envelope*. Data Encryption Standard (DES) is one of the most widely used secret key algorithms and was originally developed by IBM.

Suppose Alice wishes to send an encrypted message to Bob. She first encrypts the message with DES, using a randomly chosen DES key. Then she looks up Bob's public key and uses it to encrypt the DES key. The DES-encrypted message and the RSA-encrypted DES key together form the RSA digital envelope and are sent to Bob. Upon receiving the digital envelope, Bob decrypts the DES key with his private key, then uses the DES key to decrypt the message itself.

For authentication, in reality, RSA is combined with a hash function, such as MD5.

Suppose Alice wishes to send a signed message to Bob. She uses a hash function on the message to create a message digest, which serves as a digital fingerprint of the message. She then encrypts the message digest with her RSA private key; this is the digital signature, which she sends to Bob along with the message itself. Bob, upon receiving the message and signature, decrypts the signature with Alice's public key to recover the message digest. He then hashes the message with the same hash function Alice used and compares the result to the message digest decrypted from the signature. If they are exactly equal, the signature has been successfully verified, and he can be confident that the message did indeed come from Alice. If, however, they are not equal, then the message either originated elsewhere or was altered after it was signed, and he rejects the message.

Note that for authentication, the roles of the public and private keys are converse to their roles in encryption, where the public key is used to encrypt and the private key to decrypt. In practice, the public exponent is usually much smaller than the private exponent; this means that the verification of a signature is faster than the signing. This is desirable because a message or document will only be signed by an individual once, but the signature may be verified many times.

5.8 Dynamic Domain Name Services (DDNS)

Today's Domain Name System (DNS) servers support only queries on a statically configured database. The Dynamic DNS (DDNS) protocol defines extensions to the Domain Name System to enable DNS servers to accept requests to update the DNS database dynamically. These extensions provide support for adding and deleting a set of names and associated resource records within a single zone automatically.

The extensions assume that DNS security extensions, as defined by the IETF DNSSEC working group, have been implemented, but are not necessarily in use. DNS security extensions are used in DDNS to authenticate hosts that request to enter or change entries in the DDNS server database.

Without client authentication, another host, with perhaps malicious intent, may impersonate an unsuspecting host by remapping the address entry for the unsuspecting host to that of its own. After the remapping occurs, data (for example, logon passwords!) intended for the unsuspecting host is effectively intercepted by the malicious, spoofing host. IBM implements fail-safe RSA public-key digital signature technology to secure the DNS database updates and eliminate the possibility of spoofing. IBM is the first company to introduce products which support Dynamic DNS and associated DNS security extensions.

The following paragraphs provide a brief outline of the DDNS client and server protocol. For a more detailed explanation, please see the latest version of the IETF DNSIND and DNSSEC Internet drafts which are available online on the Worldwide Web at the following URLs:

`http://www.ietf.cnri.reston.va.us/ids.by.wg/dnsind.html`

and

`http://www.ietf.cnri.reston.va.us/ids.by.wg/dnssec.html`

DDNS Client to Server Interaction

When a DDNS client is initialized for the first time, it must be given the following information:

1. A hostname to be registered with a DDNS server
2. An IP address that goes along with that hostname
3. A default DDNS server to be updated with the given information.

The hostname could be supplied by a DHCP server; it could be chosen by a user who observes the initialization process, or it could be obtained from a configuration file which has been supplied by a system administrator. It could also be contained in an existing nameserver, of course, but that does not have to be the case. The following discussion may be helpful in finding out which technique is most suitable to your installation:

Notes:

1. Using a DHCP server to supply hostnames in addition to IP addresses will relieve a user from any involvement in the TCP/IP configuration process of his or her workstation. It will, however, place a significant burden on the administrator of the DHCP server. If a DHCP server would assign IP addresses dynamically and have hostnames go along with them, a user's hostname may change every time he or she starts TCP/IP. This will render electronic mail and other applications unusable. Moreover, if a DHCP server would store a fixed assignment of IP address and hostname per client, this could be considered a step backwards since there would be no difference to using BootP and a static Domain Name Server.
2. A better implementation of a DHCP server may, however, issue an inverse domain name query to a DDNS server to check if there is an existing mapping of a name to the IP address that the DHCP server is about to offer to a DHCP client. If this is the case, the DHCP server will include this hostname in its offer, and the DDNS client can use it to update the DDNS server accordingly.
3. If a user can choose the hostname, it may be already in use and thus be rejected by the DDNS server. In this case, the user should be given one or more attempts to enter a hostname that is not already in use. In this case, the IP address and the DDNS server name can be obtained from a DHCP server easily. This method will leave a system administrator with little or no work, since client registration will be handled by the Dynamic IP software, and the configuration of the DHCP server can be rather generic.
4. Providing a configuration file (DHCPCD.CFG) to supply a hostname for DDNS initialization will give the system administrator the option to assign hostnames to workstations but still have IP addresses assigned automatically by DHCP. This will not impede electronic mail, for instance, since that hostname is not subject to change. This method could be used for electronic software distribution environments, and it will involve some overhead to system administrators since the response files for the client installation would have to be prepared anyway. The DHCP and DDNS server configurations could be rather generic, again.

The interaction between DDNS client and server, and the role of a DHCP server in that scenario, can be summarized as follows:

1. Once the DDNS client has been provided with the required information, it will contact the name server by using the address that it has received from the

DHCP server. A user may also provide this information, along with a hostname. The client will ask that name server for the name of the primary DDNS server for this zone or domain.

2. The name server will send back the name of the primary DDNS server, which it might be itself. It is also possible to run DHCP and DDNS servers on the same system.
3. The DDNS client will then send an update request for the resource records which are associated with the client's hostname. If all goes well, the server will commit the changes to its database, and the client will be known to other hosts by the associated hostname.
4. If the specified hostname is already registered in the DDNS database with a different client, the user will be notified to enter another name.
5. Since DNS security is in place, the client will also send its public encryption key, and it will sign all resource records with a digital signature. The key and signature, together, will allow anyone to verify that it was indeed this client that created the records and that the information contained in the client's records is valid. Only that client can, later on, make changes to those records. For the purpose of maintenance, a system administrator should also have the permission to change and/or delete any resource records in the DDNS database.
6. Once the registration of a DDNS client is completed, other hosts may perform a hostname to IP address query for this client in order to send information to it.
7. A nameserver should normally also support inverse queries, or IP address to hostname mappings, so the DDNS server must be updated with that information as well. In a Dynamic IP environment, a DHCP server can carry out the job of updating a DDNS server with the inverse address resolution information for a client. This is done the following way:

   After the user has specified a hostname in the DDNS client configuration menu (which is shown in Figure 165 on page 231), and after the DDNS client has successfully registered that name with the DDNS server, the DHCP client will send a lease renewal request message to the DHCP server. The client will include the newly learned hostname in that message, thus indicating to the DHCP server that a DDNS update should occur for that information.

   The possibility of inverse name queries may also enable a DHCP server to find a hostname for a client that has not supplied one during initialization.

DDNS Message Format and Resource Records

This section provides you more detail of DDNS message format and resource records for the further understanding of the protocol and for the problem determination purpose. You may skip this section if you feel this is too detail.

DDNS Message Format

DDNS uses the domain name message format, as defined in RFC 1035, which is shown in the diagram below:

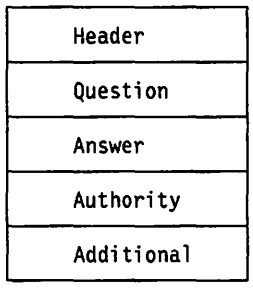


Figure 156. DDNS Message Format

The header section of a DDNS message is always present and has the following format:

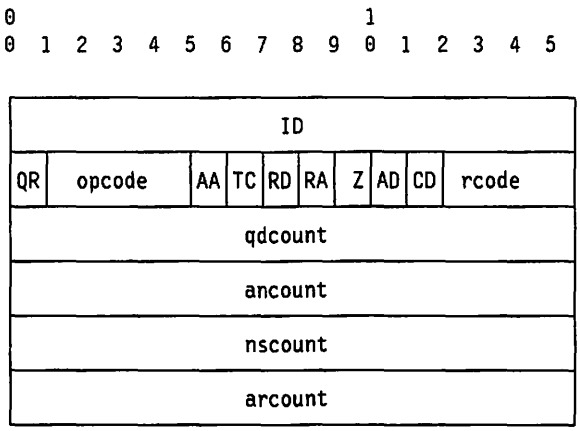


Figure 157. DDNS Message Header Format

The DDNS header format has added the AD and CD bits to the original DNS header format. The AD (authentic data) bit is used by a DDNS server to indicate that it has verified the data in a message. The CD (checking disabled) bit is used by a DDNS client to indicate that it will accept data from old DNS servers (non-verified data) as well as from secure DDNS servers.

DDNS introduces a new type of message, the UPDATE message. DDNS update messages have no section count fields, but have a new opcode (5) and new return codes (6-10) that are not known to existing static DNS servers. The following types of update requests can be distinguished:

Table 61. DDNS Update Operations

Type	Description
ADDNAMENEW	Supplies RRs with new names to be added.
ADDNAMEEXIST	Supplies RRs with existing names to be added.
ADD	Supplies RRs with new or existing names to be added.
DELETE	Specifies RRs to be deleted.
ZONEAUTHORITY	Supplies the SOA RR of the zone to be updated.

A typical DDNS transaction involves one or more update requests to the DDNS database and the processing and adding of signatures for the RRs that have been updated. Traditional DNS queries will, of course, not be subject to authentication.

DDNS Resource Records

The information that comprises a DDNS server database is represented in the form of resource records (RRs). The RR format is shown in the diagram below:

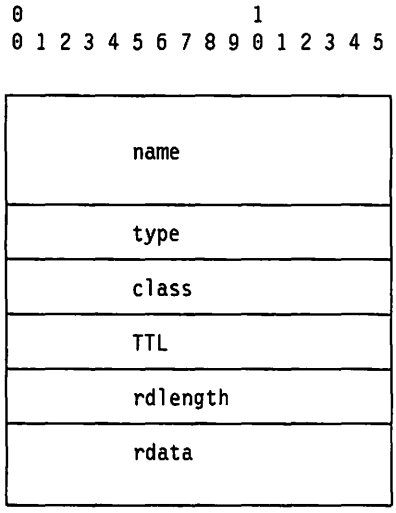


Figure 158. DDNS Resource Record Format

The implementation of the DDNS security extensions has added new types of resource records:

1. The KEY resource record (type 25).

   This record represents a public encryption key for a name in the DDNS database. This can be a key for a zone, a host or a user. A KEY RR is authenticated by SIG RR. KEY RRs contain the public exponent and modulus of an encryption key.

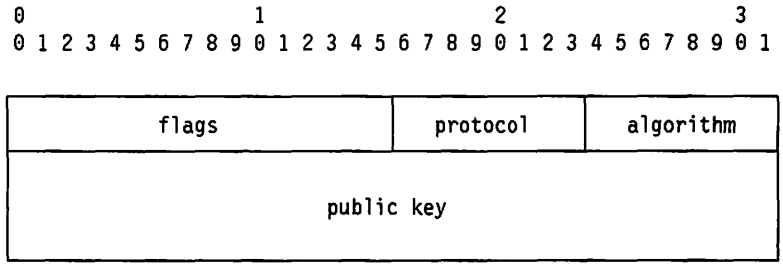


Figure 159. KEY Resource Record Format

Table 62 explains the fields used within a KEY resource record.

Table 62 (Page 1 of 2). KEY Resource Record Format

Field	Description
flags	This field indicates the type of resource record for which this KEY RR is provided.
protocol	This field indicates the protocols (in addition to DDNS) that are to be secured for authentication by this KEY RR.
algorithm	This field indicates what encryption algorithm should be used with this key; in case of IBM Dynamic IP this field has a value of 1 which means that the RSA/MD5 algorithm is being used.

Table 62 (Page 2 of 2). KEY Resource Record Format	
Field	**Description**
public key	The actual public key to be used for authentication. This field is structured in a public exponent length field, the public key exponent portion, and the public key modulus portion.

Please see the IETF Internet Draft for more details on KEY RR formats.

An exmple of a KEY resource record is shown below:

```
client1  IN   KEY   0x0000   0   1 AQO3P+UqipNXsuijeL3yyfJLw9PagI+NZg9oXrgYI1cSKOAo
                                   +WwPOxpEqUsj0hFsKNo4V0q6LH1LKl7XcytwAI01    ;Cr=auth
```

2. The SIG resource record (type 24).

   This record represents a digital signature to authenticate any resource records in a DDNS database (see 5.7, "A Short Introduction to Cryptography" on page 214 for more details on encryption and authentication). SIG RRs contain, among the digital signature itself, the type of resource record they are signing, the time until the signature will be valid, the time when the RR has been signed, and the original time to live (TTL) value for the RR they are signing.

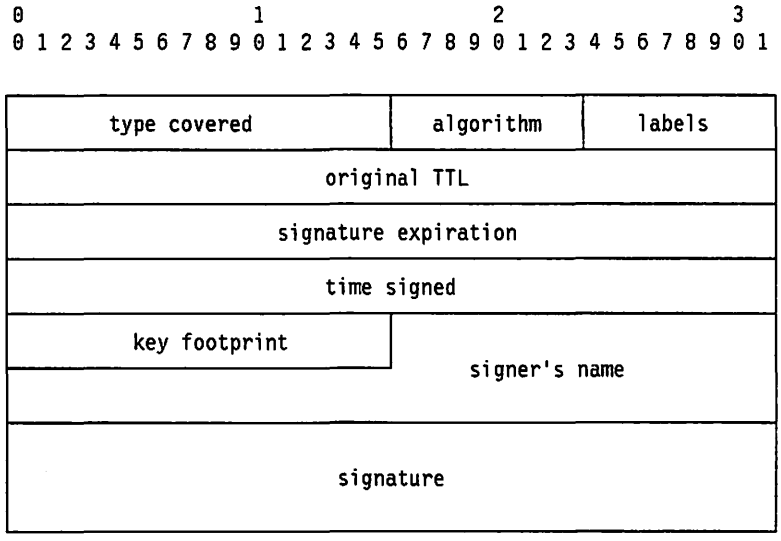

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
type covered
algorithm
labels
original TTL
signature expiration
time signed
key footprint
signer's name
signature

Figure 160. SIG Resource Record Format

Table 63 explains the fields used within a SIG resource record.

Table 63 (Page 1 of 2). SIG Resource Record Format	
Field	**Description**
type covered	This field indicates the type of RR covered by this signature.
algorithm	This field indicates what encryption algorithm should be used with this key; in case of IBM Dynamic IP this field has a value of 1 which means that the RSA/MD5 algorithm is being used.
labels	This field indicates the number of labels (host and domain name strings separated by dots) in the SIG owner name.
original TTL	The original time to live for the signed resource record is included in order to avoid caching nameservers to decrement this value. This value is protected by the signature, and it is different from the TTL of the SIG record itself.

Table 63 (Page 2 of 2). SIG Resource Record Format	
Field	**Description**
signature expiration	The time until this signature is valid. This value is represented in a number of seconds starting from 1 January 1970, GMT (ignoring leap seconds).
time signed	The time when this signature has actually been signed, represented in the same format as mentioned above.
key footprint	This field determines, depending on the applicable encryption algorithm, how to decode the signature.
signer's name	The fully qualified domain name of the signer generating this SIG RR.
signature	The actual digital signature that authenticates an RR of the type indicated in the *type covered* field.

Please see the IETF Internet Draft for more details on SIG RR formats.

An example of a SIG resource record is shown below:

```
4660   IN   SIG   KEY 1 4 4660 820470267 817356268 0x8d00 client1.test.itsc.austin.ibm.com
                                ecK2L1zhtyVnNrI24/Viitl41reduDy7TU8dxSCoGoc9zc4IIGEy4E4uVPu
                                d4fjessH8XS+H2UVjLXhr66y6Gg==     ;Cr=auth
```

To keep data traffic and memory requirements in the DDNS server as small as possible, public encryption keys and digital signatures are converted to strings using a hash function, and they are then represented in so-called base-64 format. Please see the IETF drafts for more information on the representation of KEY and SIG resource records.

Note: KEY and SIG resource records always use a single line. We have indented the examples for illustration purposes only.

5.9 Configuring an OS/2 DDNS Server

There is no explicit configuration utility for the DDNS server as there is for the DHCP server. You can either create new DDNS server configuration files, or you can migrate an existing DNS configuration to dynamic DNS server configuration files. In this section, we will show you how this can be done in both cases.

There are three ways to use the OS/2 DDNS server:

1. Static DDNS server
2. Dynamic secure DDNS server
3. Dynamic pre-secured DDNS server

When used as a static DDNS server, there is nothing you have to do but use your existing DNS configuration files with the DDNS server. It will then work exactly the same way as the previous DNS server.

When used in dynamic secure mode, the DDNS server will allow clients to update their resource records dynamically using encryption keys that have been created by the clients themselves.

When used in dynamic pre-secured mode, the DDNS server will only allow those clients to update their records to which an encryption key has been provided that has been generated at the server.

Creating a New DDNS Server Configuration

Follow the steps below to create DDNS server configuration files from scratch. The files required for a minimum configuration are:

NAMED.BT The nameserver boot file that contains the path and file names for any other configuration files. This file must be in the \MPTN\ETC\NAMEDB directory (or wherever the ETC environment variable points to). It will be examined by the DDNS server at startup.

NAMED.DOM The nameserver domain file that contains information about the zones for which this server will be authoritative, and all mappings from names to IP addresses (ordinary or forward name resolution).

NAMED.REV The nameserver reverse file that contains information about the mappings from IP addresses to names (inverse or reverse name resolution).

1. Create the \MPTN\ETC\NAMEDB directory, or create a NAMEDB directory under the directory where the ETC environment variable points to. Normally, this directory should have been created during OS/2 Warp Server installation.
2. Create the DDNS configuration files. Those files are plain ASCII files, so you can create them, for instance, with the OS/2 system editor. You can also modify the samples that are shipped with OS/2 Warp Server and contained in the \TCPIP\SAMPLES\ETC\NAMEDB directory. Normally, those sample files should also be found in the \MPTN\ETC\NAMEDB directory.

   A nameserver boot file might look as follows:

```
;
; NAMED.BT file for name server configuration.
;
; type       domain                       source file or host
;
primary  test.itsc.austin.ibm.com   f:\\mptn\\etc\\namedb\\named.dom dynamic
;
primary  200.200.200.in-addr.arpa   f:\\mptn\\etc\\namedb\\named.rev dynamic
;
```

On the `primary` statements, you can specify if you want to use the DDNS server in dynamic or in dynamic pre-secured mode by using either the `dynamic` or the `dynamic secure` keywords. A nameserver domain file might look as follows:

```
;
;*********************************
;*  Start of Authority Records  *
;*********************************
;
@   IN  SOA  ns-updates.test.itsc.austin.ibm.com.  ns-updates.test.itsc.austin.ibm.com. (
        95111601 ; Serial number for this data (yymmdd##)
        86400    ; Refresh value for secondary name servers
        300      ; Retry value for secondary name servers
        864000   ; Expire value for secondary name servers
        3600     ; Minimum TTL value
         300   ) ; dynamic update increment time
    IN  NS   ns-updates.test.itsc.austin.ibm.com.
;
localhost    IN A     127.0.0.1
;
ns-updates   IN A     200.200.200.2
martin       IN CNAME ns-updates
;
BPClient     IN A     200.200.200.14
;
```

A nameserver reverse file might look as follows:

```
;
;*********************************
;*  Start of Authority Records  *
;*********************************
;
200.200.200.in-addr.arpa.   IN  SOA  ns-updates.test.itsc.austin.ibm.com. ns-updates.test.itsc.austin.ibm.com. (
        95111601 ; Serial number for this data (yymmdd##)
        86400    ; Refresh value for secondary name servers
        300      ; Retry value for secondary name servers
        864000   ; Expire value for secondary name servers
        3600     ; Minimum TTL value
         300   ) ; dynamic update increment time

200.200.200.in-addr.arpa.  IN  NS   ns-updates.test.itsc.austin.ibm.com.
;
;
; Addresses for the canonical names
;
2          IN PTR martin.test.itsc.austin.ibm.com.
14         IN PTR BPClient.test.itsc.austin.ibm.com.
;
```

3. Start the DDNS server and ignore any messages in the following DDNSZONE command that might instruct you to stop the server.
4. After you have created the files and placed them in the \MPTN\ETC\NAMEDB directory, use the DDNSZONE command to create the public encryption key pairs for the zone resource records in the domain and reverse files.

   After the DDNSZONE command has processed the files, they may look as follows:

   - NAMED.DOM file:

```
;
;*********************************
;*  Start of Authority Records  *
;*********************************
;
@   IN  KEY     80 0 1 AQPOzUYWvAUyZhYxogDcrtxOZOH33V31TmrslDblWYiyI4Y7Mmoz6Vm3XY/QTHHOyeHcVAMKmuba+rW4/+IkMeP3
@   IN  SOA  ns-updates.test.itsc.austin.ibm.com.  ns-updates.test.itsc.austin.ibm.com. (
        95111601 ; Serial number for this data (yymmdd##)
        86400    ; Refresh value for secondary name servers
        300      ; Retry value for secondary name servers
        864000   ; Expire value for secondary name servers
        3600     ; Minimum TTL value
         300   ) ; dynamic update increment time
    IN  NS   ns-updates.test.itsc.austin.ibm.com.
;
localhost    IN A     127.0.0.1
;
ns-updates   IN A     200.200.200.2
martin       IN CNAME ns-updates
;
BPClient     IN A     200.200.200.14
;
```

- NAMED.REV file:

```
;
;*********************************
;*  Start of Authority Records  *
;*********************************
;
200.200.200.in-addr.arpa.   IN  KEY     80 0 1 AQPR+30bXCgcjmlBfKSnN4fD6vVH/AUIwincGNeDlMAuz2BTQSQ/bJkXLA3nxfV+HxKfxWp
                                        tkRckwzxEklDD3DSB
200.200.200.in-addr.arpa.   IN  SOA  ns-updates.test.itsc.austin.ibm.com. ns-updates.test.itsc.austin.ibm.com. (
        95111601 ; Serial number for this data (yymmdd##)
        86400    ; Refresh value for secondary name servers
        300      ; Retry value for secondary name servers
        864000   ; Expire value for secondary name servers
        3600     ; Minimum TTL value
         300   ) ; dynamic update increment time

200.200.200.in-addr.arpa.  IN  NS   ns-updates.test.itsc.austin.ibm.com.
;
;
; Addresses for the canonical names
;
2          IN PTR ns-updates.test.itsc.austin.ibm.com.
14         IN PTR BPClient.test.itsc.austin.ibm.com.
;
```

The DDNSZONE command will also create the DDNS.DAT file that contains the private encryption keys to sign any updates to the zone resource records in the domain and reverse files. This is shown in the following example:

```
test.itsc.austin.ibm.com ns-updates.test.itsc.austin.ibm.com
Pb7bySIfzXcWIxQ1310c9xOW6aotedZP35y/q4QzPQEpZQb215NoMbj0F1r/uA7AuQUmF2y5bcDa+gEoh7wPsXlEhZOv1Hn4Dw3Od6G/9ejG7JfugtWhjG
i2ucsd1CxFLPkUaJPNQ6gkSDPsPCVNqWrp8O8A44QxR0okSJbuq67wozjl74GUOHl9irqkQR/xUKAbEB53p6TpSYrdK4C4JQJvrSiEKhk5ntukqiOPUH24
58TsSCU0hYSX+M0sez8HSvht0+n+7HjtpTYSI2S6AG/jXuMkFjxMxUMZAOHKpky5+LPCj8f+veKa9zJ274GPClRxtBSmgwOjVTy8OylGtAkyK7Fd1V2TPA
d+4bT4vJasi2km2kGF9L+cYEVV/hoTSWwjs2n0VwfCNyl0/99vKM2CeBR4bjRZkmhsYHM8a3qb7er4ndMcNgmuZCaXJtq4THZpUdNczoP
AQPS5nBuY3404d0kWsDcjsvQSwpAKMIGNaGphB+xNKNTPsf9DMy8Lx650xQ16IcGwH/hO33VgM5CWyl3E0WDVmqz

200.200.200.in-addr.arpa ns-updates.test.itsc.austin.ibm.com
KlexSRMP/q/kkbpWEDZK9xXdBQAJNGpVktyU3QV8hAETUWDZ+uCj2siY0zYzfJKb9DhNgVVltSGyC9IE/UV+3RrPK2XvFQbEwdKdM6klUBKQXY8ymczE3J
AYeJyUedCg7604GLAoZDMGsxj5cb/sPGadizODQ6V4Hte0+Cr211N22azL5/ee8QktdOpLtmLzmZmDu94qF9i4JcyNHij1PgIFbJhl9UGMxmhTyzYZJUIc
Mwc1c1M41oUwnCNDRhON+X7TuObYfYX6wE3FsRkVADoQmn4hosLshF4VPeYOg59Z5zKS+H2a8JAZrMZfQcs7gfi1LsV3x+PHTiie/7Mzah51ChY6a2DRI7
0dSB0amfDRmbBCCxfHA1AUE2W8yxXsvKJD+auirBWygBT6B/9ZNUp6NnMrWPIcON6MTXsxpU271B41USVn6vp9MTXziyai+EAa25QMKRA=
AQPE7HDQalturlbT7Zv1nEP7318TJXv82rZX67rdVzew3Ts++KQ/ggimUPk/EodzISfYfhEyNbDcgIno9aAbqqs7
```

5. If you have a DHCP server configured for DDNS updates, you need to add the information from the DHCPSD.DAT file to the DDNS.DAT file.
6. Finally, copy the SYSLOG.CNF file from the \TCPIP\SAMPLES\ETC\NAMEDB directory to the directory that contains the nameserver files. This file configures the logging options for the DDNS server and will also be examined at server startup. Normally, it should be there already.

Note: KEY and SIG resource records as well as encryption keys always use a single line. We have indented the examples for illustration purposes only.

Migrating an Existing DNS Configuration to Dynamic IP

Before you are going to migrate a nameserver from static DNS to dynamic DDNS you should decide if you want to

- Leave existing resource records as they are and allow new ones to be created and updated dynamically. This will allow existing systems to keep their hostnames, but they will not be able to update their resource records dynamically unless a system administrator deletes them.
- Delete all existing resource records and start with a dynamic domain from the beginning.

Follow the steps below to migrate existing DNS server configuration files to Dynamic IP.

1. Modify your existing DNS configuration files (NAMED.BT, NAMED.DOM, NAMED.REV) to resemble the files as shown in the example above (before the DDNSZONE command has been run). In the case of a NAMED.BT file, you have to remove the `domain` statement, and you have to add the `dynamic` or `dynamic secure` keywords to the `primary` statements for the authoritative DNS server that you are upgrading.
2. Start the DDNS server and ignore any messages in the following DDNSZONE command that might instruct you to stop the server.
3. Use the DDNSZONE command to create the encryption keys.
4. If you have a DHCP server configured for DDNS updates, you need to add the information from the DHCPSD.DAT file to the DDNS.DAT file.
5. Copy the SYSLOG.CNF file to set DDNS server logging options.

Using a Dynamic DNS Server

To start the OS/2 DDNS server, double-click on the appropriate icon in the DDNS Services folder that is shown in Figure 161.

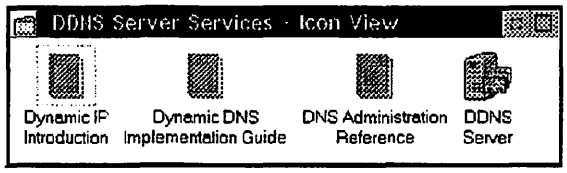


Figure 161. DDNS Services Folder

Likewise, you can start the server by entering the following command on an OS/2 command prompt:

```
NAMED
```

Figure 162 shows the OS/2 DDNS server program.

```
IBM OS/2 Warp Domain Name Server (NAMED)
          TCP/IP Version 3.1

bootfile = F:\MPTN\ETC\NAMEDB\NAMED.BT
```

Figure 162. OS/2 DDNS Server Program

To update the DDNS server database, use the following OS/2 command:

```
NSUPDATE
```

This command is also used to create cryptographic keys and to apply digital signatures. It is used by both the DHCP server and DDNS client.

To query the DDNS server database, use the following OS/2 command:

```
NSLOOKUP
```

This command works like a shell and allows you to perform subsequent queries on a nameserver.

To view the status of the DDNS server, or to take a dump of the DDNS server's database, use the following OS/2 command:

```
NSSIG
```

Note: With the former, static, version of the OS/2 DNS server, NSSIG could also be used to reload the nameserver database without taking the server down. This cannot be done with the DDNS server anymore.

5.10 Dynamic IP Client Support

The actual OS/2 client programs for DHCP and DDNS are supplied as MPTS components. OS/2 clients will also be available to other OS/2 systems as a software upgrade to the TCP/IP 3.0 for OS/2 product or component. DOS client for DHCP is provided as a part of DOS LAN Services.

Product differentiation and the value of DHCP client software lie in the ease of use and integration of DHCP clients with related networking functions. Also, as with DHCP servers, many enterprises will value the ability to customize the DHCP client to enable site-specific applications. The IBM OS/2 DHCP client is designed to operate without user intervention and provides real-time information about the client's operation through a GUI monitor application.

OS/2 Dynamic IP Clients

The Dynamic IP client programs will be installed with Adapter and Protocol Services. If you chose to use DHCP at the OS/2 Warp Server TCP/IP Services Installation menu, your TCP/IP interfaces will not be configured using the IFCONFIG command and any parameters that you have configured manually. Instead, the DHCP client will be started to get the necessary parameters from a DHCP server, and the DDNS client will be used to update the configuration of a Dynamic Domain Name Server, if one exists. Please see 5.2, "Installing TCP/IP Services" on page 171 for a more detailed description of the installation of TCP/IP Services.

The following example shows a TCP/IP initialization that resulted from using manual configuration. It is contained in the \MPTN\BIN\SETUP.CMD file, which will be executed at system start:

```
route -fh
arp -f
ifconfig lo 127.0.0.1
ifconfig lan0 200.200.200.17 netmask 255.255.255.240
route add default 200.200.200.18 1
```

The following example shows a TCP/IP initialization that resulted from selecting dynamic configuration. It is also contained in the \MPTN\BIN\SETUP.CMD file, which will be executed at system start:

```
route -fh
arp -f
dhcpstrt -i lan0
rem route add default
```

Notes:

1. DHCP interfaces must be initialized before any manually configured interfaces.
2. If multiple interfaces need to be configured dynamically, there must be a separate `dhcpstrt` statement for each of them. That means that the DHCP client must contact a server for each interface, one after the other.

The actual DHCP client program, DHCPCD.EXE, runs as a detached program since it must remain active until you shut down the system. After the TCP/IP stack has been configured with parameters that have been obtained by a DHCP server, the client has to renew the lease for that configuration as long as TCP/IP is required to be operational.

To view the current TCP/IP configuration, you can use the DHCP client monitor program that is shown in Figure 163 on page 229. You can start this program from the System Setup folder.

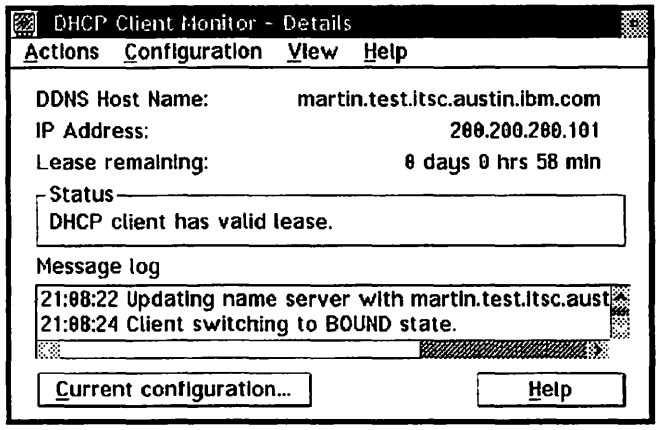


Figure 163. DHCP Client Monitor Program, Details View

If you want to review the configuration in more details, click on **Current Configuration ....** The following panel will be shown:

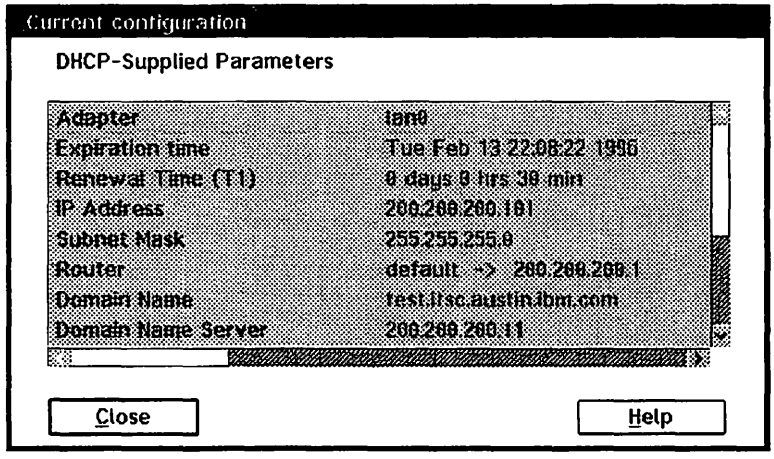


Figure 164. DHCP Client Current Configuration

Note: Starting and stopping the monitor will not affect the DHCP client.

The DHCP client can be configured by using the DHCPCD.CFG configuration file, which is normally contained in the \MPTN\ETC directory. In this file, you can specify what parameters the DHCP client should request from a server any time it is starting.

By default, the client identifies itself with its LAN adapter hardware address, and logging is enabled. Since the IBM OS/2 DHCP server allows grouping of clients that take the same set of parameters into classes, a client may want to obtain just those parameters if this workstation belongs to a certain class. This can be very helpful to separate workstations from different departments, while maintaining the capability of configuring any workstation dynamically. There is, however, administrative overhead involved since the modified configuration files

for the DHCP clients need to be supplied to the workstations during installation. Normally, this would be achieved by using electronic software distribution methods. The following example shows a default DHCPCD.CFG file:

```
# Basic options required

clientid   MAC
interface lan0

# Uncomment as desired for logging

#numLogFiles   4
#logFileSize   100
#logFileName   dhcpcd.log
#logItem       SYSERR
#logItem       OBJERR
#logItem       PROTERR
#logItem       WARNING
#logItem       EVENT
#logItem       ACTION
#logItem       INFO
#logItem       ACNTING
#logItem       TRACE

# The following are requested for interoperability with some servers which
# need explicit requests.

option 1                                # Subnet Mask
option 3                                # Router
option 6                                # Domain Name Server
option 15                               # Domain Name
option 28                               # Broadcast Address
option 33                               # Static Routes
option 60 "IBMWARP_V3.1"                # Vendor Class
option 77 "IBMWARP_V3.1"                # User Class

#updateDNS "nsupdate -h%s -d%s -s"d;a;*;a;a;%s;s;%s;3110400;q" -q"

# The following are options for which IBM supplies an installation
# script, dhcpibm.cmd, to automatically configure the IBM application
# with the served value.  Uncomment them if desired.

#option 9   exec "dhcpibm.cmd 9 %s"       # LPR Server
#option 71  exec "dhcpibm.cmd 71 %s"      # Default NewsReader/2
#option 200 exec "dhcpibm.cmd 200 %s"     # Default LPR Printer
#option 201 exec "dhcpibm.cmd 201 %s"     # Gopher Server
#option 202 exec "dhcpibm.cmd 202 %s"     # Default WWW Home Page
#option 203 exec "dhcpibm.cmd 203 %s"     # Default WWW Proxy Server
#option 204 exec "dhcpibm.cmd 204 %s"     # Default WWW News Server
#option 205 exec "dhcpibm.cmd 205 %s"     # Default Socks Server
#option 206 exec "dhcpibm.cmd 206 %s"     # NFS Servers and Mount Points
#option 207 exec "dhcpibm.cmd 207 %s"     # Default X Font Server
#option 208 exec "dhcpibm.cmd 208 %s"     # Default X System Display Manager
```

In this example, the client will identify itself using its LAN adapter hardware address (MAC) and it will use DHCP to configure one IP interface on the LAN (lan0). The client will also request specific options from a DHCP server, and it will identify itself as belonging to a certain vendor and user class. This may help a DHCP server to supply options to this client that are specific to a set of clients that form this user class.

An update string is also provided to add the client's host name resource records to a dynamic domain nameserver.

Towards the end of the configuration file, a user program can be invoked to evaluate if site-specific options have been supplied by a DHCP server. Such a program will then apply those parameters to the client's TCP/IP configuration. In case of an OS/2 WARP client, the DHCPIBM.CMD file is supplied with Adapter and Protocol Services. It is a REXX command file that evaluates site-specific

options and applies the values to the TCP/IP for OS/2 configuration. To activate this mechanism, you have to uncomment the line for one or more options in the DHCP client configuration file. Please see "Configuring Site-Specific Options for OS/2 WARP TCP/IP" on page 212 for more information on DHCP site-specific options.

When you initialize Dynamic IP for the very first time on your workstation, and a DDNS server will be used for name resolution, a host name for your workstation must be supplied. This can be done in the following ways:

1. A host name is statically defined in the name server. In this case, your host name will change whenever you receive a different IP address from the DHCP server. With Dynamic IP, this should not be an option.
2. The DHCP server will supply a host name along with an IP address. This would place a burden of work on the system administrator, and it would also mean that your host name changes when the IP address changes. That should not be the case, especially when electronic mail or NFS are being used.
3. You can choose a host name by yourself.

In the latter case, the DDNS client configuration program will be used, as shown in Figure 165. If the name you specify already exists, the name server will notify you, and you must select a different name.

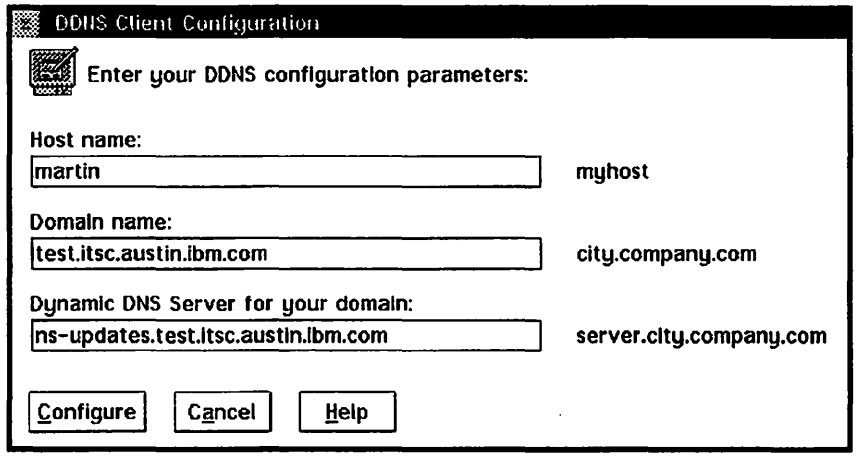


Figure 165. DDNS Client Configuration Program

The name server will store your name and the IP address that has been supplied by a DHCP server. If that address changes later, the DDNS client and DHCP server will simply update the records in the nameserver which should not involve any user interaction.

The following statement in the DHCP client configuration file includes the command that is sent to the DDNS server to update a client's A record for name resolution:

```
updateDNS "nsupdate -h%s -d%s -s"d;a;*;a;a;%s;s;%s;3110400;q" -q"
```

The %s variables will be evaluated by the DDNS client as follows:

1. Hostname
2. Domain name
3. IP address

4. Lease time

A log file is provided by the DHCP client for problem determination purposes. Logging information will normally be written to the DHCPCD.LOG file, but logging is turned off by default. An example of a DHCP client log file is shown below.

```
11/14/95 15:24:41 START:  ....log_initialize: ***************************
11/14/95 15:24:41 START:  ....log_initialize: *     NEW LOG FOLLOWS     *
11/14/95 15:24:42 START:  ....log_initialize: * ¦ ¦ ¦ ¦ ¦ ¦ ¦ ¦ ¦ ¦ ¦ ¦ ¦ *
11/14/95 15:24:42 START:  ....log_initialize: * V V V V V V V V V V V V V *
11/14/95 15:24:42 START:  ....log_initialize: ***************************
11/14/95 15:24:42 SYSERR: ....log_initialize: Logging ENABLED
11/14/95 15:24:42 OBJERR: ....log_initialize: Logging ENABLED
11/14/95 15:24:42 PROTERR:....log_initialize: Logging ENABLED
11/14/95 15:24:42 WARNING:....log_initialize: Logging ENABLED
11/14/95 15:24:42 EVENT:  ....log_initialize: Logging ENABLED
11/14/95 15:24:42 ACTION: ....log_initialize: Logging ENABLED
11/14/95 15:24:42 INFO:   ....log_initialize: Logging ENABLED
11/14/95 15:24:42 ACNTING:....log_initialize: Logging ENABLED
11/14/95 15:24:42 TRACE:  ....log_initialize: Logging ENABLED
11/14/95 15:24:42 INFO:   ....probeIfs: client has 1 previously recorded lease
11/14/95 15:24:53 INFO:   ....probeIfs: Initialized interface lan0

11/14/95 15:24:53 INFO:   ........getPortNum: dhcpc/udp unknown service, assuming port 68
11/14/95 15:24:53 TRACE:  ..........FetchHWAddress: interface 0 [802.5] physical address 08005aceea89
11/14/95 15:24:54 INFO:   ..........FetchHwType: Found the HW type for interface 0 = 6
11/14/95 15:24:54 TRACE:  ....probeIfs: [ifconfig lan0 0  broadcast 255.255.255.255]

11/14/95 15:24:54 TRACE:  ....probeIfs: ifconfig successful for 0
11/14/95 15:24:54 INFO:   ....probeIfs: Getting media ADDRESS
11/14/95 15:24:54 TRACE:  ........FetchHWAddress: interface 0 [802.5] physical address 08005aceea89
11/14/95 15:24:54 INFO:   ........FetchHwType: Found the HW type for interface 0 = 6
11/14/95 15:24:54 INFO:   ..main: number of interfaces needing DHCP configuration is 1
11/14/95 15:24:54 TRACE:  ....probeIfStatus: a previous lease (200.200.200.101 : 3600) has not yet expired
11/14/95 15:24:54 TRACE:  ......process_event: expectation fulfilled
11/14/95 15:24:54 TRACE:  ........process_fsm: generating a REQUEST
11/14/95 15:24:54 TRACE:  ........process_fsm: 6 options in Option Request List
11/14/95 15:24:54 TRACE:  ........process_fsm: generating message with xid = 682c
11/14/95 15:24:54 INFO:   ..........getPortNum: dhcps/udp unknown service, assuming port 67
11/14/95 15:24:54 TRACE:  ..........transmitMailbox: transmitting to (200.200.200.11 #67)
11/14/95 15:24:54 INFO:   ..........process_timer: Ta Seconds = 30
11/14/95 15:24:55 TRACE:  ........process_fsm: state transition to REBOOTING
11/14/95 15:24:55 TRACE:  ........SelectFunc: DHCP comm descriptor selected
11/14/95 15:24:55 TRACE:  ......client_event: received packet xid = 682c
11/14/95 15:24:55 INFO:   ........primeOptions: Option: 53, length:1
11/14/95 15:24:55 INFO:   ........primeOptions: Option: 58, length:4 value: 134676480 (0x08070000)
11/14/95 15:24:55 INFO:   ........primeOptions: Option: 59, length:4 value: 1309409280 (0x4e0c0000)
11/14/95 15:24:55 INFO:   ........primeOptions: Option: 54, length:4 value: 197707976 (0x0bc8c8c8)
11/14/95 15:24:55 INFO:   ........primeOptions: Option: 1, length:4 value: 16777215 (0x00ffffff)
11/14/95 15:24:55 INFO:   ........primeOptions: Option: 3, length:4 value: 29935816 (0x01c8c8c8)
11/14/95 15:24:55 INFO:   ........primeOptions: Option: 6, length:4 value: 197707976 (0x0bc8c8c8)
11/14/95 15:24:55 INFO:   ........primeOptions: Option: 15, length:24
11/14/95 15:24:55 INFO:   ........primeOptions: Option: 51, length:4 value: 269352960 (0x100e0000)
11/14/95 15:24:55 INFO:   ........primeOptions: Option: 72, length:4 value: 197707976 (0x0bc8c8c8)
11/14/95 15:24:55 TRACE:  ........legibleReply: DHCP message type DHCPACK
11/14/95 15:24:56 TRACE:  ....receiveEvent: Expecting xid 682c  , Got xid 682c
11/14/95 15:24:56 TRACE:  ......process_event: expectation fulfilled
11/14/95 15:24:56 TRACE:  ........process_fsm: Checking address for clash.
11/14/95 15:24:56 TRACE:  ..........arpcheck: deleting old arp entry.
11/14/95 15:24:56 TRACE:  ..........arpcheck: sending pings.
11/14/95 15:24:57 TRACE:  ..........arpcheck: checking arp table.
11/14/95 15:24:57 ACTION: ........process_fsm: announcing the new IP address 200.200.200.101 obtained from server
11/14/95 15:24:57 ACTION: ..........record_offer: recorded offer (200.200.200.101 : 3600) from server 200.200.200
11/14/95 15:24:57 INFO:   ..........record_offer: Pseudo T2 limit set to 22
11/14/95 15:24:57 INFO:   ..........record_offer: Pseudo T3 limit set to 1 interval 300
11/14/95 15:24:57 INFO:   ............count_option_match: Counted 4 matches in offer from 200.200.200.11.
11/14/95 15:24:58 INFO:   ..........updateLeaseRecord: t1 is 1800
11/14/95 15:24:58 INFO:   ..........updateLeaseRecord: t2 is 60
11/14/95 15:24:58 ACTION: ........process_fsm: Using lease (200.200.200.101 : 3600) from server 200.200.200.11
11/14/95 15:24:58 TRACE:  ........process_fsm: Plugboard starts now...

11/14/95 15:24:58 TRACE:  ..........SetOptions: Inside SetOptions
11/14/95 15:24:58 INFO:   ..........SetOptions: ddnscfg verification: domain test.itsc.austin.ibm.com
11/14/95 15:24:58 TRACE:  ............exec_set_ipaddress: ip address = 200.200.200.101
11/14/95 15:24:58 TRACE:  ............exec_set_ipaddress: cmd = ifconfig lan0 netmask 200.200.200.101
11/14/95 15:24:58 INFO:   ..........SetOptions: Option 1 received
11/14/95 15:24:58 TRACE:  ..........SetOptions: running builtin_exec for 1.
11/14/95 15:24:58 TRACE:  ............exec_set_mask: cmd = ifconfig lan0 netmask 255.255.255.0
11/14/95 15:24:59 INFO:   ..........SetOptions: Option 3 received
11/14/95 15:24:59 TRACE:  ..........SetOptions: running builtin_exec for 3.
11/14/95 15:24:59 TRACE:  ............exec_set_routes: SetOptions: Route option
```

```
11/14/95 15:24:59 TRACE:  ..........exec_set_routes: Router Option command is = route add default 200.200.200.1 1
11/14/95 15:25:00 INFO:   ..........route_add: dest 0 router c8c8c801 type GATEWAY
11/14/95 15:25:00 INFO:   .........SetOptions: Option 6 received
11/14/95 15:25:00 TRACE:  .........SetOptions: running builtin_exec for 6.
11/14/95 15:25:00 TRACE:  ..........exec_set_dns_server: SetOptions: Domain Name Option
11/14/95 15:25:00 TRACE:  ..........exec_set_dns_server: Domain = [test.itsc.austin.ibm.com]

11/14/95 15:25:01 INFO:   .........SetOptions: Option 15 received
11/14/95 15:25:01 INFO:   .........SetOptions: Option 51 received
11/14/95 15:25:01 INFO:   .........SetOptions: Option 53 received
11/14/95 15:25:01 INFO:   .........SetOptions: Option 54 received
11/14/95 15:25:01 INFO:   .........SetOptions: Option 58 received
11/14/95 15:25:01 INFO:   .........SetOptions: Option 59 received
11/14/95 15:25:01 INFO:   .........SetOptions: Option 72 received
11/14/95 15:25:01 INFO:   .........SetOptions: Option 255 received
11/14/95 15:25:01 ACTION: ........process_fsm: assigned net address 200.200.200.101 to interface 0
11/14/95 15:25:02 TRACE:  ........process_fsm: state transition to BOUND
```

In the example above, you can see a DHCP client that has already been configured. It will therefore start with a DHCPREQUEST message and then enter REBOOTING state. After the server has replied with a DHCPACK message, the configuration parameters will applied to the client's TCP/IP configuration. In fact, this example matches the DHCP server log file example that is shown in 211.

When the OS/2 Dynamic IP client has been initialized, it will store the options received from the DHCP and DDNS servers in the \MPTN\ETC\DHCPC.DB file and it will also modify the original DHCPCD.CFG file. The client will attempt to request the stored information again whenever it is restarted.

DLS Dynamic IP Clients

DOS LAN Services has a DHCP support code built in when you install DLS. However, you should explicitly select DHCP during the installation.

5.11 Operational Scenario of Dynamic IP

This section provides several scenarios for simple and complex DHCP/DDNS configurations with some considerations to multiple DHCP server environment.

Simple Dynamic IP Scenario

This section will provide an example for a very simple Dynamic IP scenario involving only a client and a server on a single IP subnet. This is shown in Figure 166 on page 234.

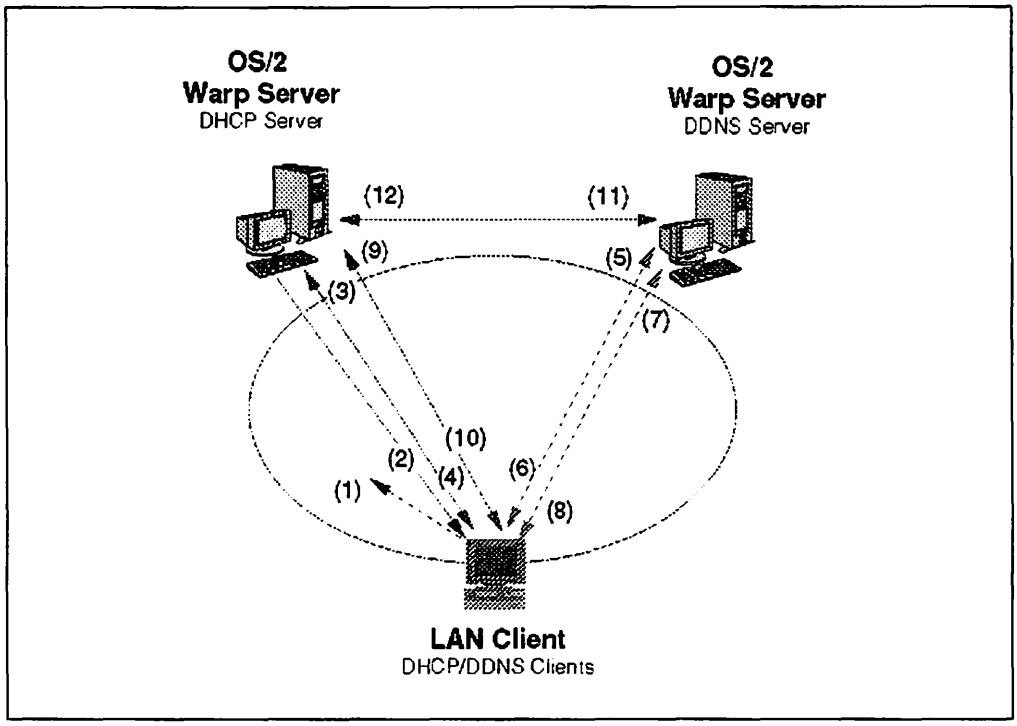


Figure 166. Simple Dynamic IP Scenario

For a very simple scenario, the DHCP and DDNS servers in the figure above would be on the same OS/2 Warp Server system. We have separated those functions only for a better illustration of the Dynamic IP operation.

The following steps describe the Dynamic IP operation in the scenario shown above, when the client is started for the first time:

1. DHCPDISCOVER, broadcast by the DHCP client
2. DHCPOFFER, sent by the DHCP server containing configuration options
3. DHCPREQUEST, broadcast by the DHCP client
4. DHCPACK, sent by the DHCP server
5. DNS query for primary nameserver, sent by the DDNS client
6. DNS authoritative reply, sent by the DDNS server
7. DDNS update query, sent by the DDNS client containing the hostname specified by the user
8. DDNS acknowledgement, sent by the DDNS server
9. DHCPREQUEST lease renewal, sent by the DHCP client supplying the hostname specified by the user
10. DHCPACK, sent by the DHCP server
11. DDNS update query, sent by the DHCP server to update the DDNS database with the inverse mapping information for the hostname and IP address
12. DDNS acknowledgement, sent by the DDNS server

The following example shows the DHCP server and DDNS server configuration files used in this scenario:

- DHCPSD.CFG file (DHCP server):

```
numLogFiles          4
logFileSize          100
logFileName          dhcpsd.log
leaseTimeDefault     1 hours
leaseExpireInterval  10 minutes
supportBOOTP  no
supportUnlistedClients  yes
logItem      SYSERR
logItem      OBJERR
logItem      PROTERR
logItem      WARNING
logItem      EVENT
logItem      ACTION
logItem      INFO
logItem      ACNTING
logItem      TRACE
#.indent 12

updateDNS "nsupdate -f -r%s -s"d;ptr;*;a;ptr;%s;s;%s;0;q""

network     200.200.200.0  200.200.200.1-200.200.200.20    #.name Test Network
{
    #.ddns 200.200.200.10
    client 0 0 200.200.200.1    #.exclu
    client 0 0 200.200.200.10    #.exclu
    option 3       200.200.200.1    #.name 3 Router
    option 6       200.200.200.10    #.name 6 Domain Name Server
    option 15       test.itsc.austin.ibm.com    #.name 15 Domain Name
    option 201       200.200.200.10     #.name 201 - Gopher Server
}
```

- NAMED.BT file:

```
;
; NAMED.BT file for name server configuration.
;
; type       domain                      source file or host
;
primary  test.itsc.austin.ibm.com    c:\\mptn\\etc\\namedb\\named.dom dynamic
;
primary  200.200.200.in-addr.arpa    c:\\mptn\\etc\\namedb\\named.rev dynamic
;
```

- NAMED.DOM file:

```
$ORIGIN itsc.austin.ibm.com.
test        IN      KEY     0x0080   0   1 AQPS5nBuY3404d0kWsDcjsvQSwpAKMIGNaGphB+xNKNTPsf9DMy8Lx650xQ16lcGwH/h033
                                           VgM5CWyl3E0WDVmqz ;Cl=5
            IN      SOA     ns-updates.test.itsc.austin.ibm.com. ns-updates.test.itsc.austin.ibm.com. (
            95112502 86400 300 864000 3600 300 )    ;Cl=5
            IN      NS      ns-updates.test.itsc.austin.ibm.com.    ;Cl=5
$ORIGIN test.itsc.austin.ibm.com.
martin      IN      CNAME   ns-updates.test.itsc.austin.ibm.com.    ;Cl=5
localhost   IN      A       127.0.0.1       ;Cl=5
client1     IN      KEY     0x8000   0   1 AQO3P+UqipNXsuijeL3yyfJLw9PagI+NZg9oXrgYI1cSKOAo+WwPOxpEqUsj0hFsKNo4V0q
                                           6LH1LKl7XcytwAI01 ;Cr=auth
    4660    IN      A       200.200.200.2   ;Cr=auth
    4660    IN      SIG     A 1 4 4660 817359867 817356267 0x8d00 client1.test.itsc.austin.ibm.com tDCJdEVGFPTPAt8
                            nN+0z3lu0FgWhomCORcKaY3xhBbJalnLvF0KmG+D//JJ+7RmM+rqrW9AK7qQslvlyum6NPw== ;Cr=auth
    4660    IN      SIG     KEY 1 4 4660 820470267 817356268 0x8d00 client1.test.itsc.austin.ibm.com ecK2L1zhtyVnN
                            rl24/Viitl41reduDy7TU8dxSCoGoc9zc4IIGEy4E4uVPud4fjessH8XS+H2UVjLXhr66y6Gg==   ;Cr=auth
ns-updates  IN      A       200.200.200.10  ;Cl=5
```

- NAMED.REV file:

```
$ORIGIN 200.200.in-addr.arpa.
200             IN      KEY     0x0080   0   1 AQPE7HDQalturlbT7ZvlnEP7318TJXv82rZX67rdVzew3Ts++KQ/ggimUPk/EodzISfYfhE
                                               yNbDcgIno9aAbqqs7 ;Cl=5
                IN      SOA     ns-updates.test.itsc.austin.ibm.com. ns-updates.test.itsc.austin.ibm.com. (
                95112502 86400 300 864000 3600 300 );Cl=5
                IN      NS      ns-updates.test.itsc.austin.ibm.com.;Cl=5
$ORIGIN 200.200.200.in-addr.arpa.
2               IN      KEY     0x0080   0   1 AQPvxnJUi6hiHzRJC/beIJDsfFtumzD2He33CvM5mY0PMGTYVk0YR+DUNTtdlG0wm20NFvo
                                               5uVAOdRdIuIMfb4UN ;Cr=auth
        4660    IN      PTR     client1.test.itsc.austin.ibm.com.  ;Cr=auth
        4660    IN      SIG     PTR 1 4 4660 817430323 817426724 0x856f 2.200.200.200.in-addr.arpa sPfLnGeDm9i+N/jyLDn
                                VRPl8tKTYMQT2zsf135nqFRR+AyrZrCPSEICA4UmK8787IQXMmcawczAj0UgrNgtllA==     ;Cr=auth
        4660    IN      SIG     KEY 1 4 4660 817430323 817426724 0x856f 2.200.200.200.in-addr.arpa vnsYFxdSJNQl+YmheIk
                                fxvZ1Ia3jeyMuS7YOPyTcVH7bqXJgoys1elvvmMgGYEBHb+YU3lyt2tZARqpA+FfQeQ==     ;Cr=auth
10              IN      PTR     ns-updates.test.itsc.austin.ibm.com. ;Cl=5
```

- SYSLOG.CNF file:

```
numLogFiles     4
logFileSize     100
logFileName     syslog.
logItem         LOG_EMERG
logItem         LOG_ALERT
logItem         LOG_CRIT
logItem         LOG_ERR
logItem         LOG_WARNING
logItem         LOG_NOTICE
logItem         LOG_INFO
```

- DHCPCD.CFG file (DHCP client):

```
# Basic options required

clientid   MAC
interface lan0

# Uncomment as desired for logging

numLogFiles   4
logFileSize   100
logFileName   dhcpcd.log
logItem       SYSERR
logItem       OBJERR
logItem       PROTERR
logItem       WARNING
logItem       EVENT
logItem       ACTION
logItem       INFO
logItem       ACNTING
logItem       TRACE

# The following are requested for interoperability with some servers which
# need explicit requests.

option 1                                # Subnet Mask
option 3                                # Router
option 6                                # Domain Name Server
option 15                               # Domain Name
option 28                               # Broadcast Address
option 33                               # Static Routes
option 60 "IBMWARP_V3.1"                # Vendor Class
option 77 "IBMWARP_V3.1"                # User Class

#updateDNS "nsupdate -h%s -d%s -s"d;a;*;a;a;%s;s;%s;3110400;q" -q"

# The following are options for which IBM supplies an installation
# script, dhcpibm.cmd, to automatically configure the IBM application
# with the served value.  Uncomment them if desired.

#option 9   exec "dhcpibm.cmd 9 %s"       # LPR Server
#option 71  exec "dhcpibm.cmd 71 %s"      # Default NewsReader/2
#option 200 exec "dhcpibm.cmd 200 %s"     # Default LPR Printer
#option 201 exec "dhcpibm.cmd 201 %s"     # Gopher Server
#option 202 exec "dhcpibm.cmd 202 %s"     # Default WWW Home Page
#option 203 exec "dhcpibm.cmd 203 %s"     # Default WWW Proxy Server
#option 204 exec "dhcpibm.cmd 204 %s"     # Default WWW News Server
#option 205 exec "dhcpibm.cmd 205 %s"     # Default Socks Server
#option 206 exec "dhcpibm.cmd 206 %s"     # NFS Servers and Mount Points
#option 207 exec "dhcpibm.cmd 207 %s"     # Default X Font Server
#option 208 exec "dhcpibm.cmd 208 %s"     # Default X System Display Manager
```

Notes:

1. KEY and SIG resource records as well as encryption keys always use a single line. We have indented the examples for illustration purposes only.
2. You will realize that the format of the NAMED.DOM and NAMED.REV files looks quite different from the examples shown in "Creating a New DDNS Server Configuration" on page 223. This format will be used after the first update has occurred to the DDNS server, no matter what the format has been before, so you don't have to worry about it. Both formats will work, but only the second one will actually be used.

Complex Dynamic IP Scenario

This section will provide an example for a more complex Dynamic IP scenario involving a client and a server on different IP subnets and also involving a Bootp client and a BootP relay agent. This is shown in Figure 167 on page 238.

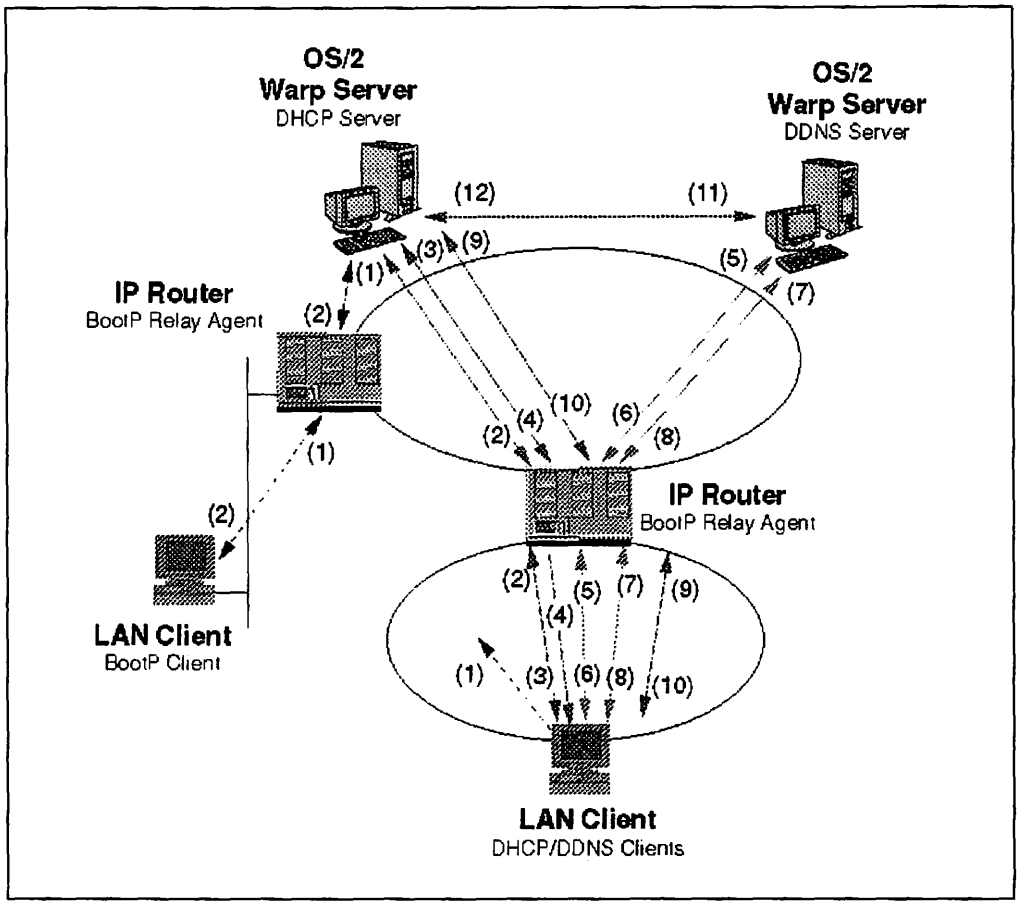


Figure 167. Complex Dynamic IP Scenario

The following steps describe the Dynamic IP operation in the scenario shown above, when the Dynamic IP client is started for the first time:

1. DHCPDISCOVER, broadcast by the DHCP client on the local subnet and forwarded by the BootP relay agent in the IP router
2. DHCPOFFER, sent by the DHCP server containing configuration options and forwarded by the BootP relay agent in the IP router
3. DHCPREQUEST, broadcast by the DHCP client on the local subnet and forwarded by the BootP relay agent in the IP router
4. DHCPACK, sent by the DHCP server and forwarded by the BootP relay agent in the IP router
5. DNS query for primary nameserver, sent by the DDNS client
6. DNS authoritative reply, sent by the DDNS server
7. DDNS update query, sent by the DDNS client containing the hostname specified by the user
8. DDNS acknowledgement, sent by the DDNS server
9. DHCPREQUEST lease renewal, sent by the DHCP client supplying the hostname specified by the user
10. DHCPACK, sent by the DHCP server
11. DDNS update query, sent by the DHCP server to update the DDNS database with the inverse mapping information for the hostname and IP address

12. DDNS acknowledgement, sent by the DDNS server

The following steps describe the BootP operation in the scenario shown above, whenever the BootP client is started:

1. BootP request, broadcast by the BootP client on the local subnet and forwarded by the BootP relay agent in the IP router
2. BootP reply, sent by the DHCP server containing configuration options and forwarded by the BootP relay agent in the IP router

Using Multiple Dynamic IP Servers

The following considerations should be made when you want to install multiple Dynamic IP servers for backup purposes:

1. The address ranges of DHCP servers must not overlap.
2. DHCP servers do not communicate or consolidate their configurations between each other.
3. DHCP servers can support multiple subnets.
4. Only one DDNS server can be authoritative for a domain and can accept update requests.

You can still provide at least some functional backups in the following ways:

1. Distribute IP addresses of one or more subnets across multiple DHCP servers. If one server fails, only the range of IP addresses that this server was managing will be unavailable. Just make sure that you do not overlap IP address ranges when you are setting up multiple DHCP servers.
2. Use secondary nameservers. If the primary DDNS server fails, no more update requests can be processed in this zone, but the latest available database will be held in secondary nameservers to answer queries. However, if the primary server is down for a longer time than the resource records in the secondaries' databases are valid, the whole zone will gradually become unavailable.

5.12 Interoperability with OEM and Legacy Hosts

As mentioned earlier, a benefit of Dynamic IP using only open networking standards is that IBM products interoperate with OEM IP networking products. More specifically, Dynamic IP clients may be served by OEM DHCP and DNS servers. Dynamic IP DHCP servers may serve OEM BootP or DHCP clients. Dynamic IP DNS servers are a functional superset of existing DNS servers and may be seamlessly inserted into existing customer DNS server hierarchies.

Connecting Windows NT Clients to an OS/2 DHCP Server

When you install Windows NT 3.5 with Microsoft TCP/IP support, or when you configure Microsoft TCP/IP on Windows NT at a later time, you can choose to manually configure TCP/IP parameters or use DHCP. Figure 168 on page 240 shows the TCP/IP configuration menu of a Windows NT system.

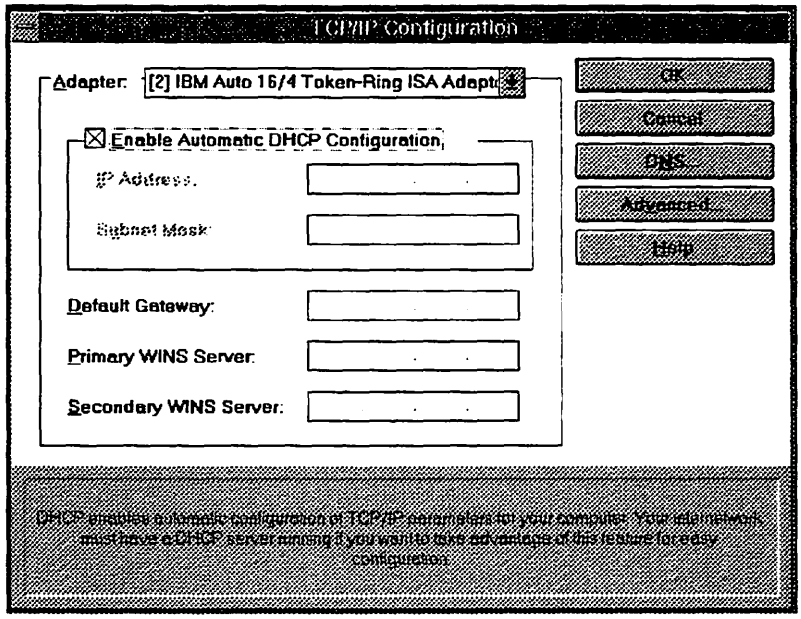


Figure 168. Windows NT TCP/IP Configuration

We have successfully connected a Windows NT DHCP client to the IBM OS/2 DHCP server. Windows NT cannot participate in DDNS.

Connecting Windows 95 Clients to an OS/2 DHCP Server

When you install Windows 95 with Microsoft TCP/IP support, or when you configure Microsoft TCP/IP on Windows 95 at a later time, you can choose to manually configure TCP/IP parameters or use automatic configuration (DHCP). Figure 169 shows the TCP/IP configuration menu of a Windows 95 system.

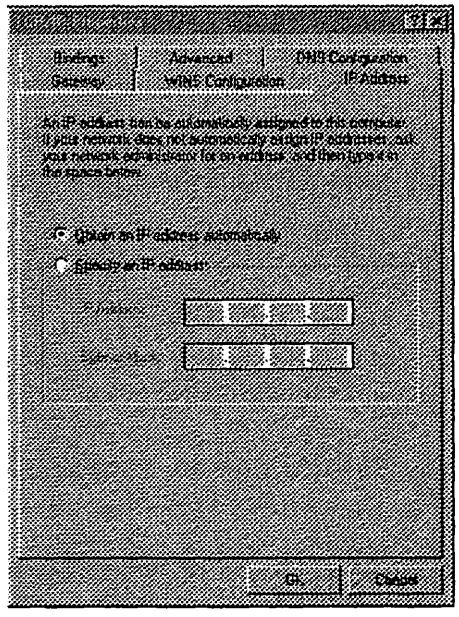


Figure 169. Windows 95 TCP/IP Configuration

We have successfully connected a Windows 95 DHCP client to the IBM OS/2 DHCP server. Windows 95 cannot participate in DDNS.

Connecting IBM Dynamic IP Clients to Windows NT DHCP Server

A Windows NT 3.5 Advanced server system offers a DHCP server to be installed as an option of Microsoft TCP/IP support. Figure 170 shows the DHCP server configuration menu of a Windows NT system.

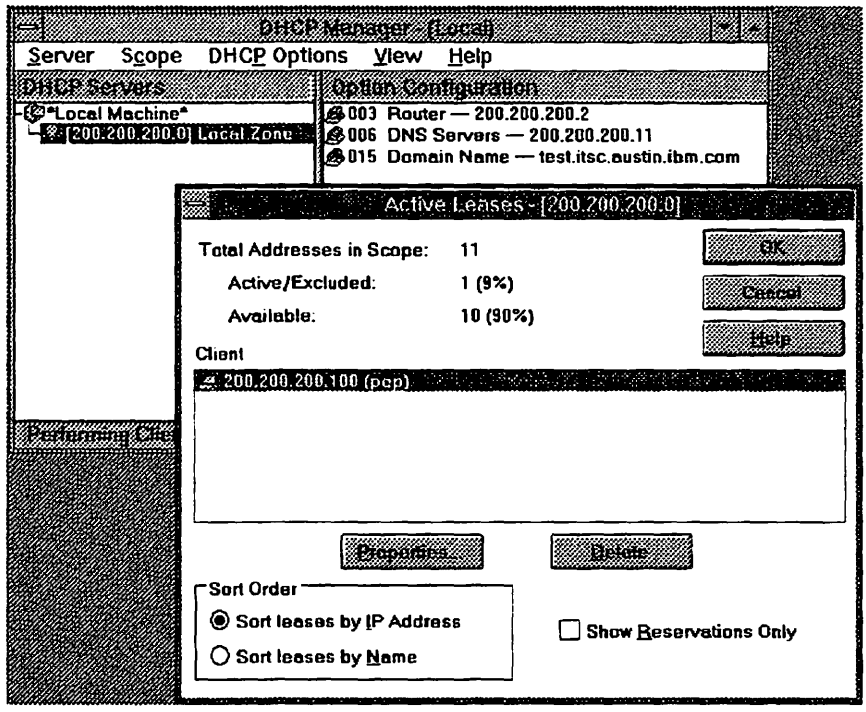


Figure 170. Windows NT DHCP Server Configuration

We have successfully connected the OS/2 DHCP client to a Windows NT DHCP server.

Windows NT also uses the Windows Internet Name Service (WINS), for which it supplies client and server programs. This service works as a nameserver for NetBIOS over TCP/IP P-node, M-node, and H-node systems, providing a mapping service from NetBIOS names to IP addresses. WINS works in a dynamic way that is similar to DDNS, but it does not provide any client authentication. WINS also cannot be used as a nameserver in the DNS hierarchy.

Please refer to Chapter 6, "NetBIOS over TCP/IP (TCPBEUI)" on page 259 for more information on NetBIOS over TCP/IP discussions.

5.13 Accessing the Internet with OS/2 Warp Server

This section describes the following options to provide Internet access for, and with your, OS/2 Warp Server system:

- Register as a new Internet user
- Accessing the Internet from the OS/2 Warp Server system via the IBM Internet Connection for OS/2
- Sharing a communications port and modem over the LAN so that other workstations can access the Internet via your OS/2 Warp Server system

You can, of course, also access the Internet over a LAN attachment via your company's Internet gateway, if one exists and, if you are authorized to use it.

Figure 171 shows the Internet services available to your OS/2 Warp Server system.

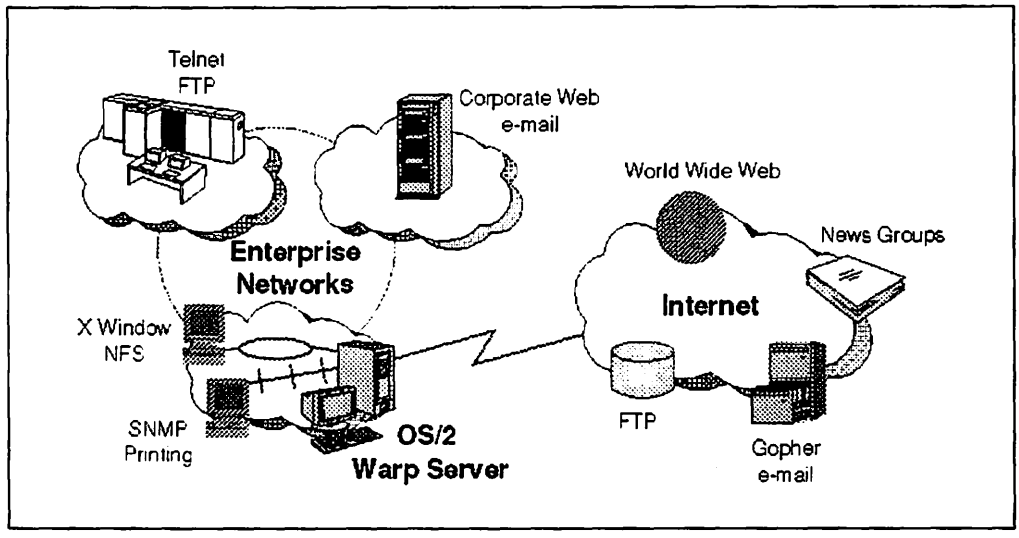


Figure 171. OS/2 Warp Server LAN and Internet Connectivity

Internet Registration

If you want to use IBM as your Internet service provider, you can use the registration utility that is provided with the TCP/IP Services to register yourself as an Internet user. Open the Internet Connection folder on your OS/2 Desktop; then open the Internet Customer Services folder, and double-click on the Registration icon. After reading the short introduction and the terms and conditions that apply to the IBM Internet Connection for OS/2, you will need to fill in the account owner information.

Note: You need a valid major credit card in order to open an Internet account with the IBM Internet Connection for OS/2.

Figure 172 on page 243 shows the Internet account registration.

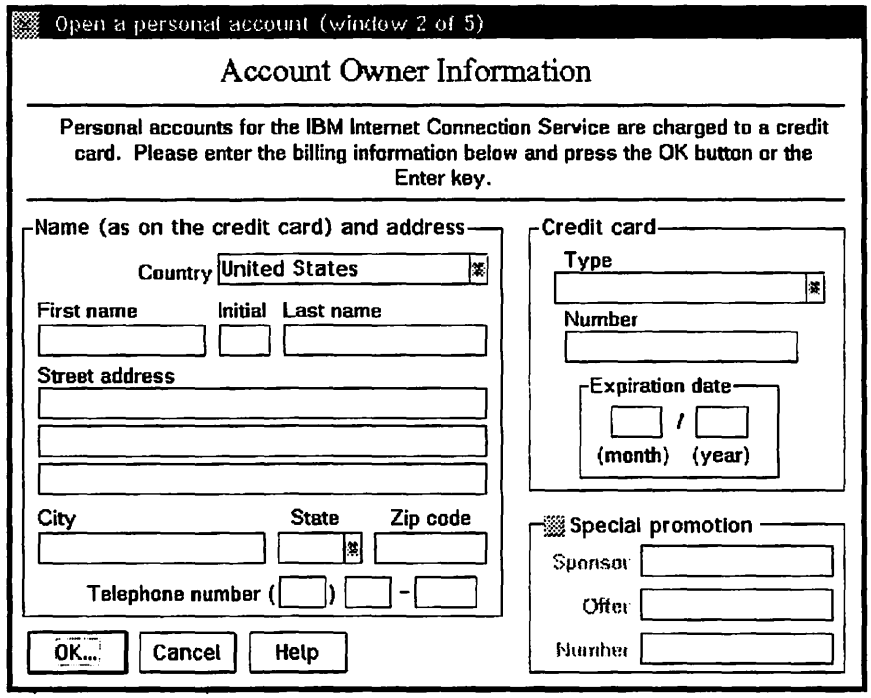


Figure 172. Internet Account Registration

After filling out the account information, you can select a modem type and COM port for your attachment, and you can choose the appropriate telephone number to dial IBM Internet registration in your country.

With the Customer Assistance application contained in the IBM Internet Customer Services folder, you can later change or delete your registered account. You can also add more user IDs to this account, thus providing Internet access for a group of people within your company. Figure 173 on page 244 shows the IBM Internet Customer Assistance application.

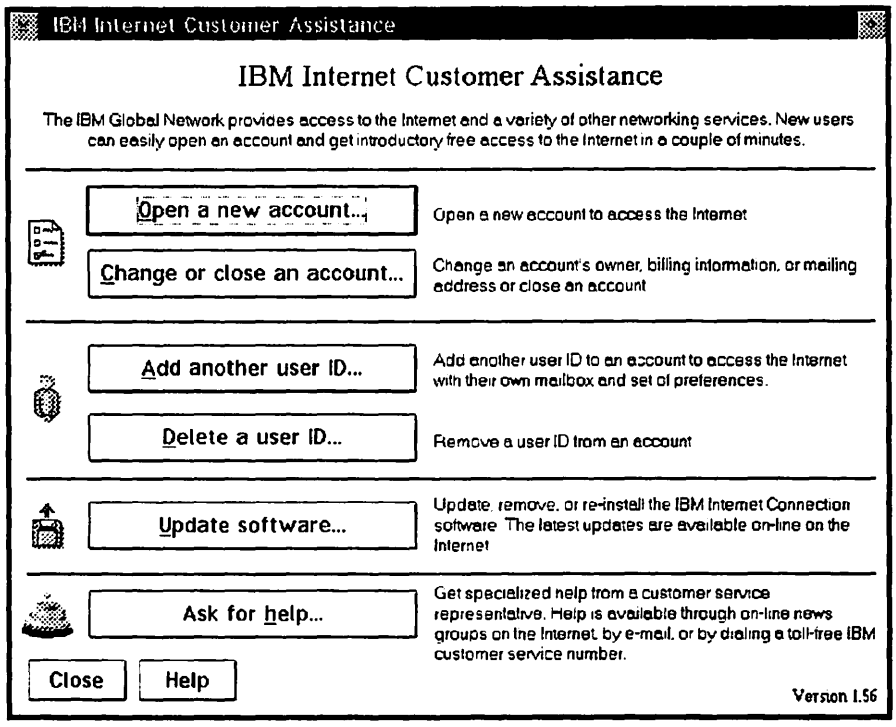

IBM Internet Customer Assistance
IBM Internet Customer Assistance
The IBM Global Network provides access to the Internet and a variety of other networking services. New users can easily open an account and get introductory free access to the Internet in a couple of minutes.
Open a new account...
Open a new account to access the Internet
Change or close an account...
Change an account's owner, billing information, or mailing address or close an account
Add another user ID...
Add another user ID to an account to access the Internet with their own mailbox and set of preferences.
Delete a user ID...
Remove a user ID from an account
Update software...
Update, remove, or re-install the IBM Internet Connection software. The latest updates are available on-line on the Internet
Ask for help...
Get specialized help from a customer service representative. Help is available through on-line news groups on the Internet, by e-mail, or by dialing a toll-free IBM customer service number.
Close
Help
Version 1.56

Figure 173. IBM Internet Customer Assistance Application

Using IBM Internet Connection for OS/2

Once you are registered to the IBM Internet Connection, you can use the following TCP/IP applications from your Internet Connection folder or from the Internet Utilities folder contained therein:

- WebExplorer
- Gopher
- News Reader
- Telnet
- FTP
- 3270 Telnet

When you start any of these applications by double-clicking on the appropriate icon, the Internet Dialer will be invoked automatically to let you dial-up to your configured Internet service provider before the application is actually started. Figure 174 on page 245 shows the Internet Dialer application.

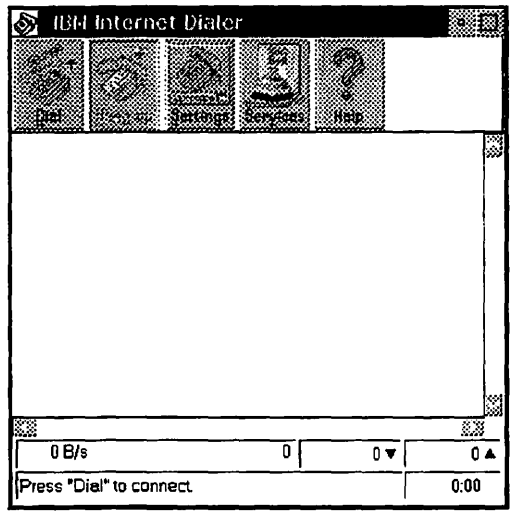


Figure 174. IBM Internet Dialer Application

When you click on **Settings**, you will see the Internet Dialer Settings notebook as shown in Figure 175.

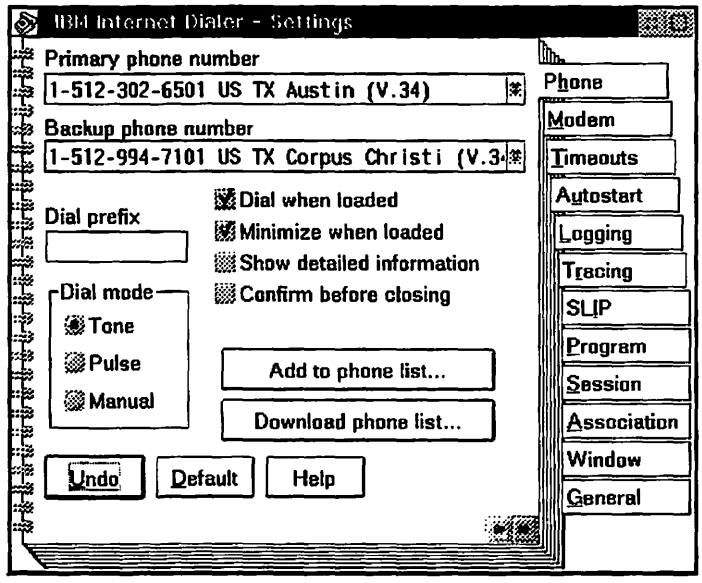


Figure 175. IBM Internet Dialer Settings Notebook

When you have finished configuration, you can log onto the IBM Global Network from the panel shown in Figure 176 on page 246.

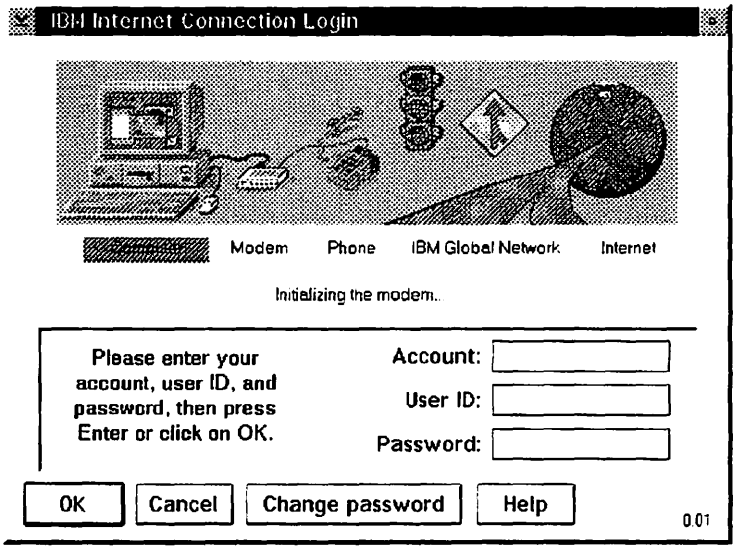


Figure 176. IBM Internet Connection Login Panel

Another very useful feature is the capability to retrieve the latest version of programs for your Internet Connection, called Retrieve Software Updates.

If you do not want to use IBM as your Internet service provider, the Internet Connection gives you dial access to other service providers as well.

5.14 Expanding OS/2 Warp Server TCP/IP Capabilities

Apart from the TCP/IP functions and services that are contained in OS/2 Warp Server and which have been described earlier, there are more TCP/IP features that you might want to add to your OS/2 Warp Server system. The following sections will describe how you can expand OS/2 Warp Server's TCP/IP capabilities by adding NFS, the X Window System and Internet server components, and we will also tell you what you need in order to develop your own applications based on TCP/IP for OS/2.

Those add-ons were originally available as additional kits for IBM TCP/IP V2.0 for OS/2. In order to use them with the TCP/IP Services of OS/2 Warp Server, you may have to apply additional corrective services or program fixes about which we will inform you, where appropriate.

Network File System (NFS) Services

NFS enables you to share disk drives or directories across TCP/IP networks as if the resources were local. It uses Remote Procedure Calls (RPC) for communication between clients and servers. You can add NFS capability to an OS/2 Warp Server system by installing the *Network File System kit*. This will provide you with the following functions:

- NFS client
- Mounting NFS drives from remote hosts, including UNIX, MVS, OS/2, and other systems
- NFS server
- PCNFSD support for the NFS server
- Query an NFS server for exported directories
- Create and maintain a PASSWD file for PCNFSD

The NFS kit integrates itself into the TCP/IP configuration notebook to simplify configuring NFS components together with other features of TCP/IP Services.

Note: NFS does not support extended file attributes which are common in OS/2.

To run an NFS client with OS/2 Warp Server requires that you also install the corrective service diskette (CSD) package UN57064 of the NFS kit. Make sure you install the original NFS kit before you install the CSD. You do not have to reboot between the two installation processes.

If you experience an error while installing the NFS kit, copy the TCPINST.EXE, TCPINST2.EXE, TCPINST.HLP, and UNZIP.DLL files as well as the entire \LANLK subdirectory from the CSD diskette to the original NFS kit diskette, and restart the installation program.

To run an NFS server with OS/2 Warp Server requires that you install CSD UN57064 and that you additionally apply the APAR PN69745 program fix.

To obtain CSDs and APAR fixes for the NFS kit, please contact IBM Service or your local IBM representative. You may also receive those fixes by anonymous FTP from `ftp.software.ibm.com`.

Figure 177 shows a functional diagram of NFS.

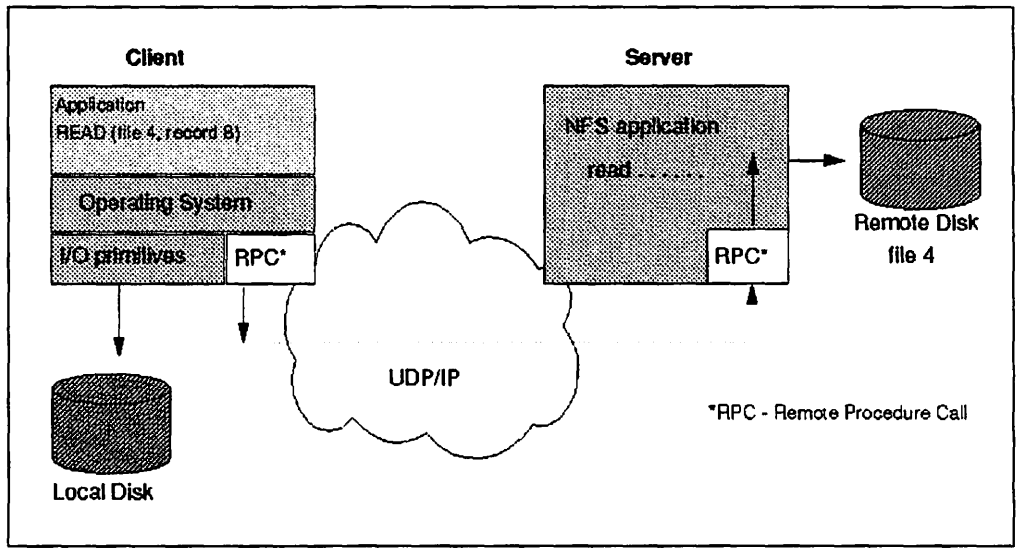


Figure 177. Network File System

To start the OS/2 NFS client program, click on its icon in the TCP/IP folder, or enter the following command on an OS/2 command prompt:

```
NFSSTART
```

Figure 178 on page 248 shows the OS/2 NFS client program.

```
IBM TCP/IP OS/2 NFS Client Release (May 11 1994)
Copyright (c) IBM Corp. 1993.  All rights reserved.
Buffer size:     8192
RPC timeout:     1 seconds.
No. of retries:  5
No. of Biods:    4
Priority:  class:4 level:1
Parallel Read requests:  on
Parallel Write requests:         off
Respect case when creating files/directories:    on
Case sensitive comparisons:      on
File creation permission bits: 700, directory creation permission bits: 700
UMASK for accessing files: 600
NFS BIOD 1 running
NFS BIOD 2 running
NFS BIOD 3 running
NFS BIOD 4 running

NFS Control Program Running.
```

Figure 178. OS/2 NFS Client Program

To start the OS/2 NFS server program, you have to start the Portmapper program first by entering the following command on an OS/2 command prompt:

```
PORTMAP
```

Then, start the NFS server by entering the following command on an OS/2 command prompt:

```
NFSD
```

Figure 179 shows the OS/2 NFS server program.

```
NFSD    IBM OS/2 NFS Server Version 1.2 (Feb 06 1995)

Reading the exports file...
Registering MOUNTD with portmap...
NFS: Warning: Environment variable TZ is not set.
Registering NFSD with portmap...
NFS: File ownership set to uid 0, gid 0.
NFSD: Initialization complete.  Server running.
```

Figure 179. OS/2 NFS Server Program

X Window System Server

The *X Window System Server (PMX) kit* enables you to display and control X Window System client applications in one or multiple OS/2 Presentation Manager (PM) windows. PMX is an implementation of the X11R5 version of the X Window System and offers features such as backing-store and pseudo-color support using PM palette manager.

Because PMX uses OS/2 PM as the window manager, it supports all of the keyboard, display and pointer devices that are supported by OS/2 PM, and it can also use native PM fonts (but not DBCS fonts).

The PMX kit also integrates itself into the TCP/IP configuration notebook to simplify configuring PMX components together with other features of TCP/IP Services.

Note: To run a PMX server with OS/2 Warp Server requires that you also install the corrective service diskette (CSD) package UN68122 of the PMX kit.

If the PMX kit is installed via C.I.D., and you have placed CSD UN68122 files in the same directory where the original PMX files or any earlier CSD files are located at the server, you may encounter a bad return code from the installation process (rc=2 or rc=6) at the client. In this case, you should apply APAR PN70086.

To obtain CSDs and APAR fixes for the PMX kit, please contact IBM Service or your local IBM representative. You may also receive those fixes by anonymous FTP from `ftp.software.ibm.com`.

Figure 180 shows PMX displaying an X Window application on the OS/2 Desktop. The application is actually executed on an RS/6000 running AIX.

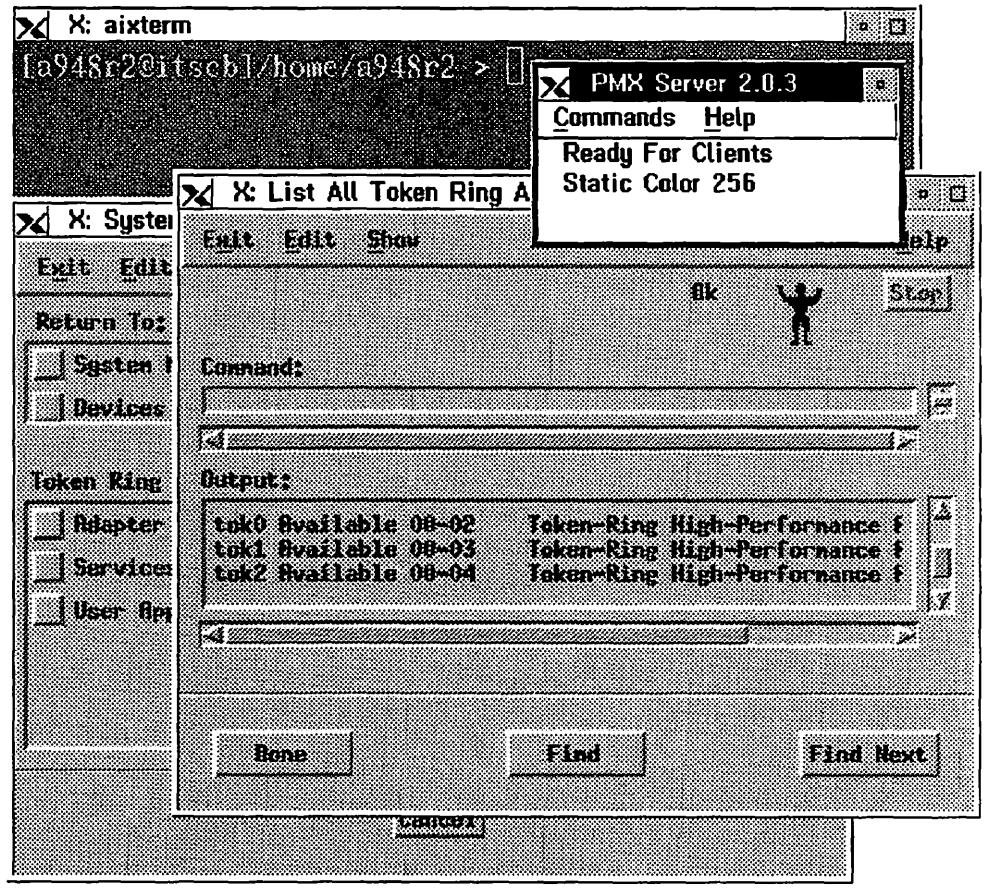


Figure 180. X Window System Server

IBM Internet Connection Server for OS/2 Warp

A business can effectively promote its corporate messages, provide marketing information, give sales support to customers, and even gain a competitive edge by having their own home pages accessible on the Web. Access to the Web pages can be kept within a company or made available outside of the company. The *Internet Connection Server for OS/2 Warp* provides all the necessary features to get Web pages on the Internet, and offers the following services:

- Acts as a repository for resources (home pages) created with Hypertext Markup Language (HTML).
- Serves requests from a Web browser (client) using Hypertext Transfer Protocol (HTTP) to transfer the document.
- Provides proxy support, which means the server acts as an agent for the browser to access remote servers not directly accessible by the browser because of security access restrictions. The proxy server supports requests from HTTP, FTP and Gopher and acts on their behalf.
- Supports proxy caching. The proxy server can temporarily store files, which makes subsequent requests for those files available to the requester much quicker.
- Provides application interfaces using Common Gateway Interface (CGI) which is an API between the Web server and another application such as a database. Sample CGI scripts are provided that will negotiate the movement of data between the Web server and an outside application.
- Provides a quick and easy installation. Web server is installed using the standard OS/2 installation tool, Software Installer.
- An easy-to-use configuration tool is provided. HTML forms are used to configure such information as time-out settings, proxy servers and caching. The OS/2 WebExplorer can be used for configuration and administration tasks.
- In order to support national languages, the Web Server is also DBCS enabled.

The Internet Connection Server for OS/2 is part of the IBM Internet Connection family which includes servers and browsers for several IBM operating systems as well as network services, Web site hosting and Internet consulting. The Internet Connection Server for OS/2 will also be enhanced to support the Secure HTTP (S-HTTP) and Secure Sockets Layer (SSL) protocols in the near future, and there will be gateway components between the Web server and IBM legacy applications, such as CICS OS/2 and DB2/2.

Figure 181 on page 251 gives an overview of the IBM Internet Connection family.

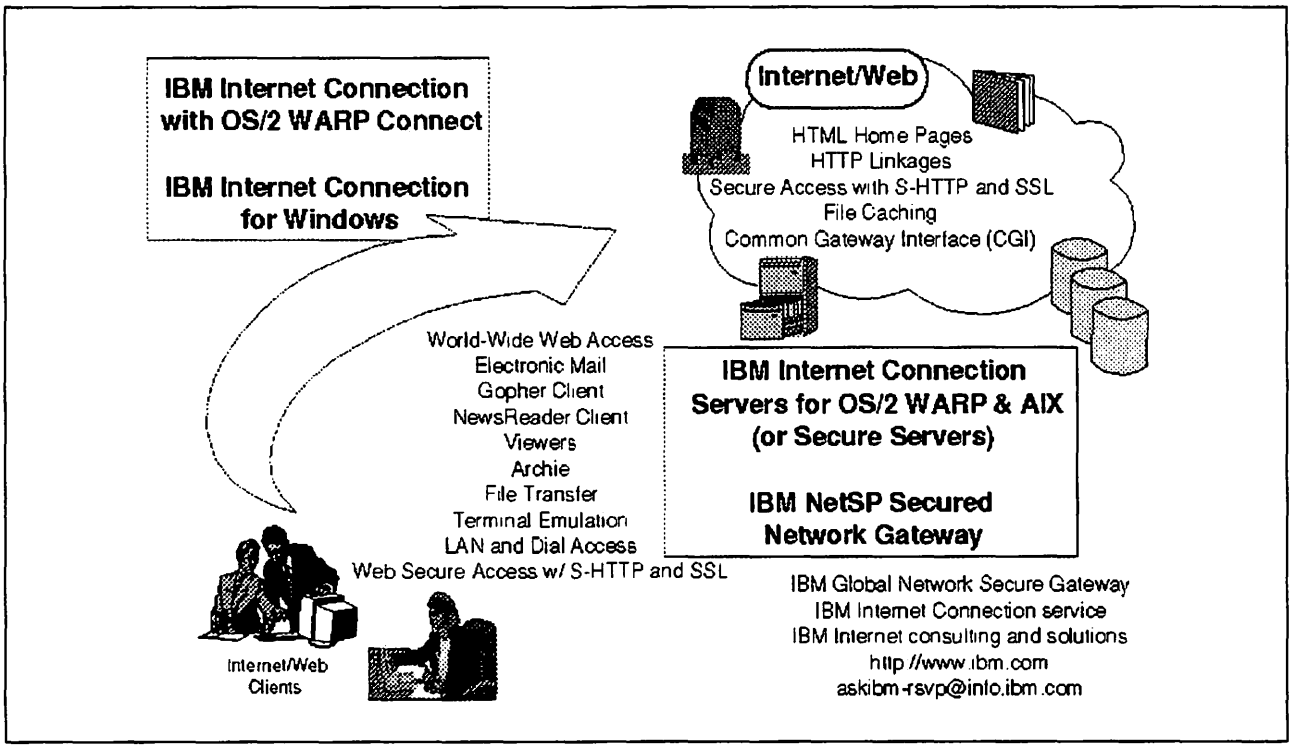


Figure 181. IBM Internet Connection Family

Figure 182 on page 252 shows WebExplorer displaying an HTML page off an IBM Internet Connection Server for OS/2.

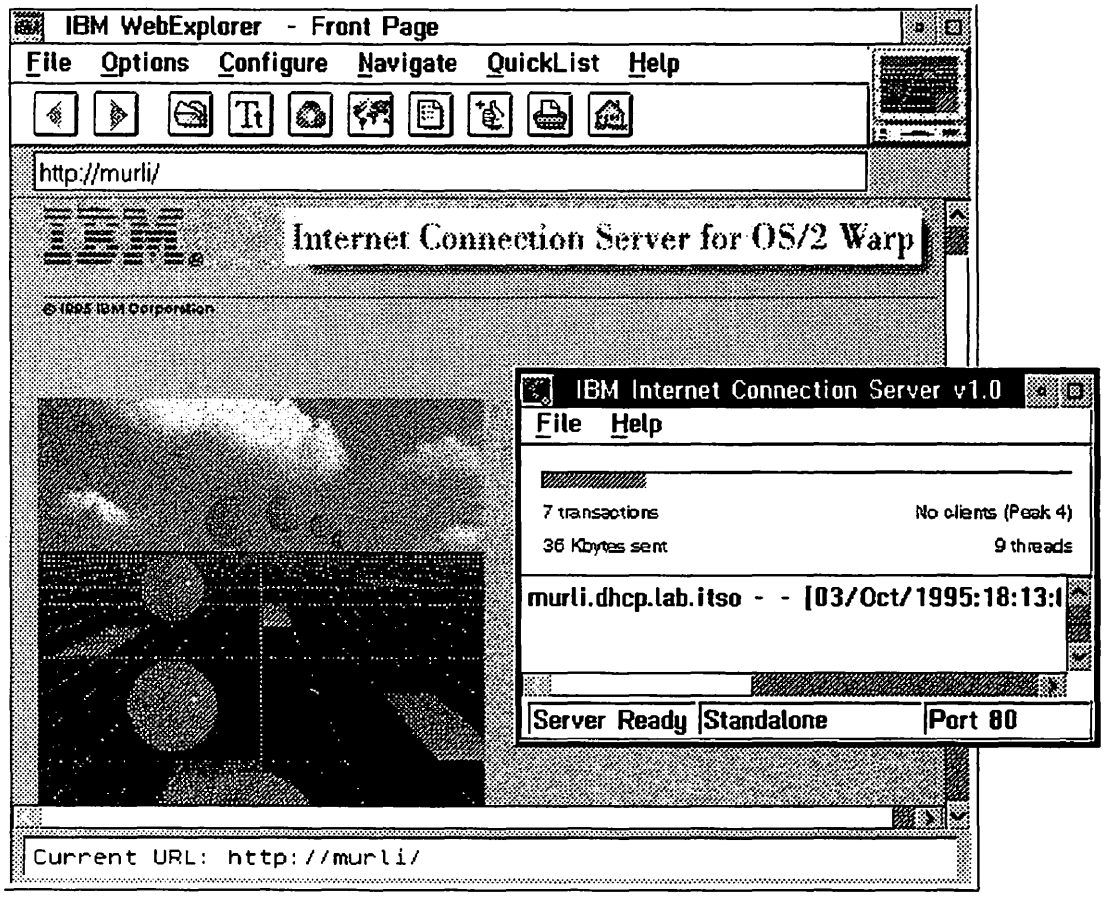


Figure 182. Internet Connection Server for OS/2

Enabling TCP/IP Services for Secure Firewall Access Using Socks

One may say that the Internet is great because there is so much information out there that can be accessed very easily and quickly. Electronic communication has become a lot easier because of the Internet, no doubt, but it can also be a dangerous thing at times. Imagine that someone would get into your system and destroy data at random just because you forgot to implement a preventive security system. Or, worse, imagine someone would tap into your system, learn your passwords and then use your account information to do electronic shopping.

There are certainly other ways of compromising information on the Internet, so how can you protect your system?

Firewalls

One way to deal with network security is the installation of a specialized server, a so-called *firewall*. It prevents unauthorized traffic in and out of a secure network and addresses only TCP/IP-accessible networks. Normally, one would dedicate a network machine that does not run other applications. Figure 183 on page 253 shows the operation of a firewall.

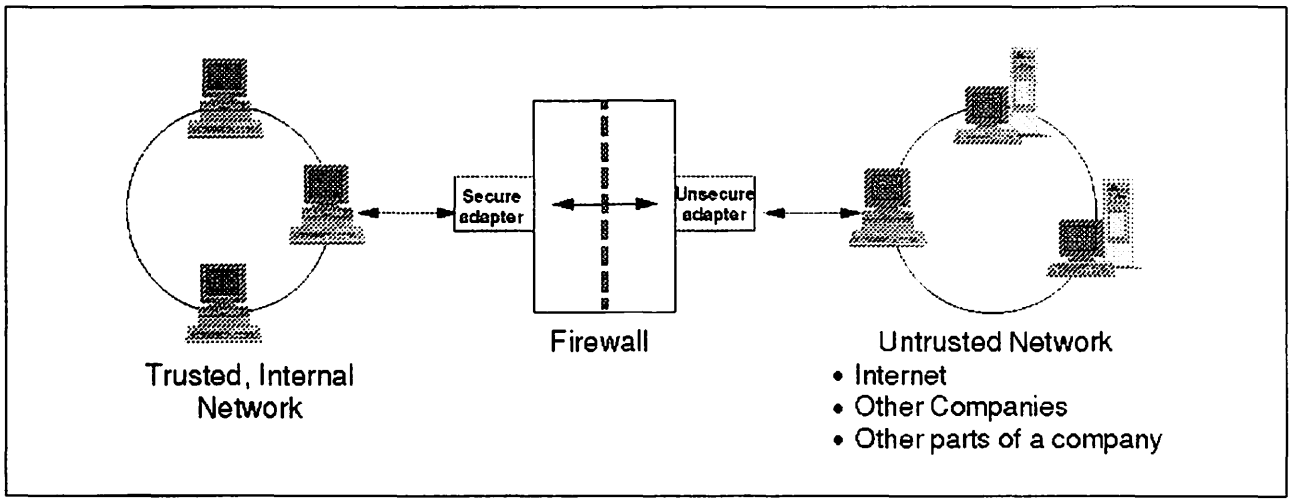


Figure 183. Firewall Operation

To provide maximum security, a good firewall design is paramount, and includes properties such as:

- Anything not explicitly permitted should default to denied
- Increasing complexity leads to bugs, which lead to opportunities
- Server should be kept in a physically secure environment
- Provide extensive logging
- Turn off known problems and non-essential daemons (applications and services)

Most of the firewalls available today offer one or more of the following services:

- Filtering gateways
- Proxy application layer gateways
- Circuit layer gateways (Socks servers)
- Domain Name Server hiding
- Mail handling
- Audit and logging

Multiple technologies are needed to provide capabilities and protection. The NetSP Secure Network Gateway (SNG), for instance, is based on IBM's technology and has been used for seven years to protect internal IBM networks.

Socks API

Socks is intended to provide secure access from a trusted network into an unsecure network. Though Socks is presently specified in an IETF Internet draft only, it is already regarded as a de-facto standard. Socks uses a specialized version of an application, a so-called *socksified* version which is using a special API to interface with TCP and UDP. With Socks, access permit/deny rules may be based on IP addresses, TCP and UDP port numbers, and/or a list of user IDs.

The application code for Socks runs on client systems, not on a firewall, so there is less load on the firewall machine. This turns out to be useful when resource intensive applications, such as Mosaic, are frequently used. Socks support can be implemented for multiple applications, such as WWW, FTP, Telnet, and others.

In contrast to application proxy gateways (which act on behalf of a client to get access to an unsecure network), Socks requires a sockisfied version of a client

application; proxy gateways do not. On the other hand, application proxy gateways use password authentication which is not required for Socks.

Socks will be available for the TCP/IP 3.0 for OS/2 product or as a component update. Figure 184 shows the operation of a Firewall with the Socks interface.

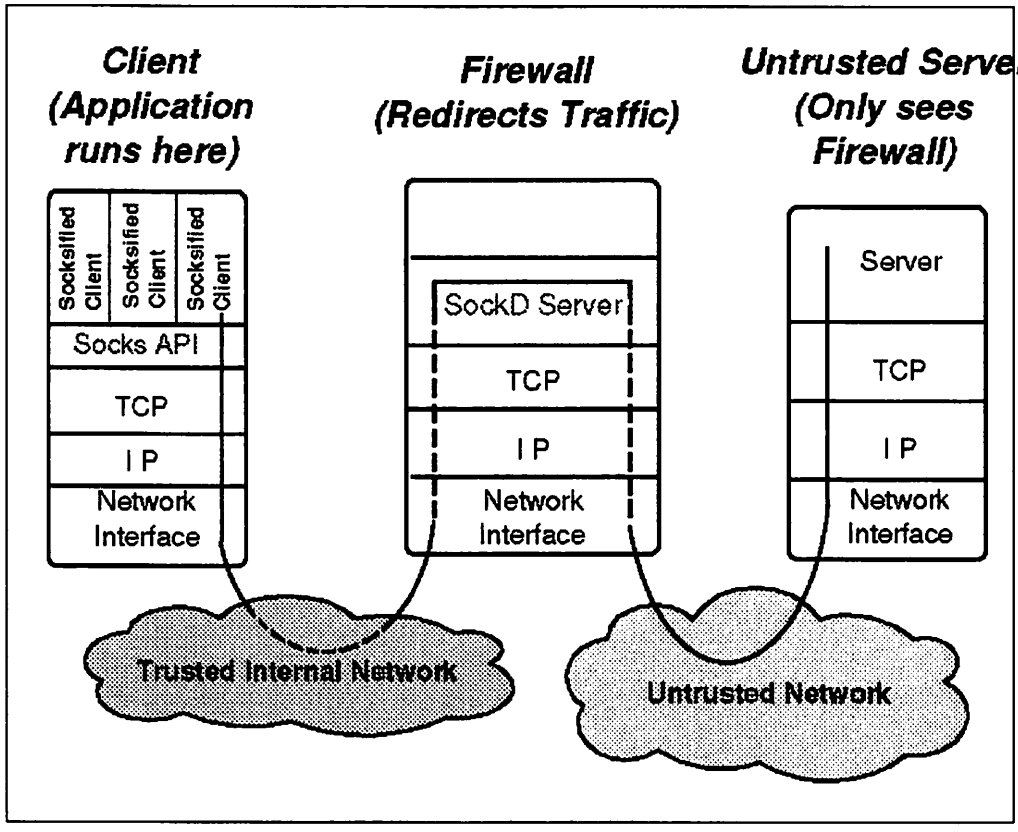


Figure 184. Firewall and Socks

Developing Your Own TCP/IP Applications

Apart from the REXX programming interfaces to the Sockets and FTP APIs that are included in TCP/IP Services, there are several packages available for you to develop your TCP/IP applications under OS/2. Depending on what type of program you want to create, you may choose from the following:

Programmer's Toolkit: The Programmer's toolkit provides routines, libraries and header files for application programming on TCP/IP for OS/2. It includes support for the Sockets, RPC, and FTP APIs, and the SNMP distributed programming interface (DPI). This kit requires a 32-bit ANSI C-compiler, such as IBM C Set/2 Version 1.0, or later.

X Window System Client Kit: The X Window System Client kit consists of two components:

1. The X Window System Client Runtime Services
2. The X Window System Client Programmer's Toolkit

These components provide the standard X Window System APIs from the MIT Consortium, enabling users to write X Window applications for OS/2 or to port X Window System applications from other platforms. The kit also enables the running of such applications by providing DLLs for the APIs and some utilities to

support the X Window applications. This kit requires the Programmer's Toolkit for application development and the X Window System Server kit to run X Window Client applications on OS/2.

OSF Motif Kit: The OSF/Motif kit consists of two components:

1. The OSF/Motif Runtime Services
2. The OSF/Motif Programmer's Toolkit

These components provide the standard OSF/Motif Athena widgets and header files, enabling users to write and run Motif applications on OS/2. The OSF/Motif kit requires the X Window System Client kit and the Programmer's Toolkit.

Adding Wide Area Network (WAN) Connectivity to TCP/IP Services

The *Extended Networking kit* will provide an IP interface to X.25 and SNA LU6.2 networks.

Notes:

1. The Extended Networking kit requires OS/2 Communications Manager (CM/2) for the base X.25 and SNA LU6.2 support. You should use version 1.11 of CM/2, along with the latest fixes for OS/2 Warp, or a later version.
2. The version of CM/2 that is included in the Attach Pak for OS/2 Warp does not include X.25 support.
3. To run the Extended Networking kit with OS/2 Warp Server, we recommend that you also install the corrective service diskette (CSD) package UN60005 of the Extended Networking kit.

To obtain CSDs and APAR fixes for the Extended Networking kit, please contact IBM Service or your local IBM representative. You may also receive those fixes by anonymous FTP from `ftp.software.ibm.com`.

5.15 Supporting DOS and Windows Applications with TCP/IP Services

OS/2 Warp Server allows DOS and Windows applications that are using either the WinSock 1.1 or the IBM TCP/IP 2.1.1 for DOS APIs to communicate over a network by using the TCP/IP protocol stack that comes with OS/2 Warp Server itself.

A virtual device driver will play the role of a DOS TCP/IP protocol stack and then forward any application requests to TCP/IP for OS/2. The support files for the DOS and WIN-OS/2 environment are kept under the \TCPIP\DOS directory. Sample PING (DOS) and WPING (Windows) applications are also provided. They are located in the \TCPIP\DOS\BIN directory.

Figure 185 on page 256 shows a functional diagram of DOS and Windows application support provided by TCP/IP Services.

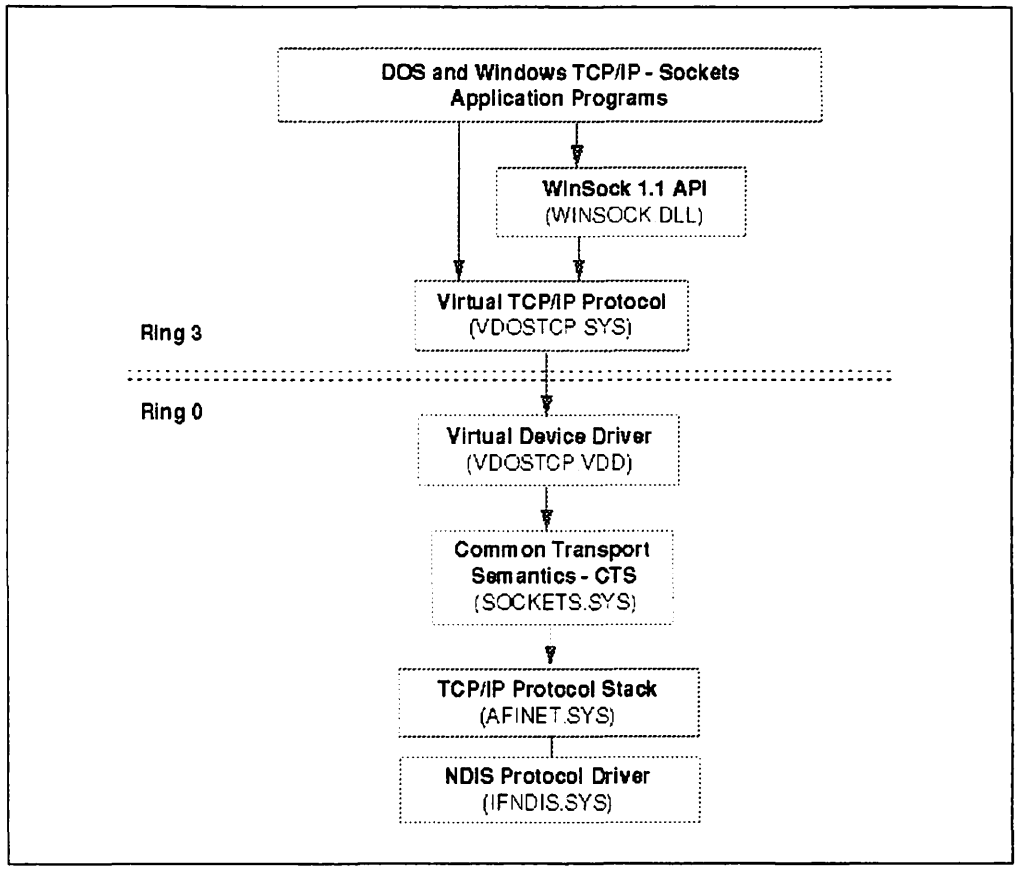

DOS and Windows TCP/IP - Sockets Application Programs
WinSock 1.1 API (WINSOCK DLL)
Virtual TCP/IP Protocol (VDOSTCP SYS)
Ring 3
Ring 0
Virtual Device Driver (VDOSTCP VDD)
Common Transport Semantics - CTS (SOCKETS.SYS)
TCP/IP Protocol Stack (AFINET.SYS)
NDIS Protocol Driver (IFNDIS.SYS)

Figure 185. TCP/IP DOS and Windows Application Support

5.16 TCP/IP Client and Server Functions

This section provides a brief summary of IBM TCP/IP client and server functions available today on the OS/2 platform. If a function is included in OS/2 Warp Server, no additional packages are required, as indicated in Table 64.

Table 64 (Page 1 of 2). OS/2 Warp Server TCP/IP Services

TCP/IP function	Client	Server	Add-on package required
Telnet	Yes	Yes	No
Telnet PM	Yes	Yes (TelnetD)	No
Telnet 3270	Yes	n/a	No
Telnet 5250	Yes	n/a	No
FTP	Yes	Yes	No
FTP PM	Yes	Yes (FTPD)	No
TFTP	Yes	Yes	No
REXEC	Yes	Yes	No
RSH	Yes	Yes	No
LPR/LPD	Yes	Yes	No

Table 64 (Page 2 of 2). OS/2 Warp Server TCP/IP Services			
TCP/IP function	**Client**	**Server**	**Add-on package required**
LPRMON	Yes	Yes (LPD)	No
LPRPORTD	Yes	Yes (LPD)	No
Portmapper	n/a	Yes	No
SMTP	Yes	Yes	No
Multimedia Mail	Yes	Yes	No (IBM TCP/IP V2.0 for OS/2 UltiMail Kit included in TCP/IP Services)
TALK	Yes	Yes	No
Gopher	Yes	No	No
World Wide Web	Yes	Yes	IBM Internet Connection Server for the server function
NewsReader/2	Yes	No	No
DOS/Windows access	Yes	Yes	No (IBM TCP/IP V2.0 for OS/2 DOS/Windows Access Kit included in TCP/IP Services)
SLIP	Yes	Yes	No
PPP	Yes	Yes	No
Finger	Yes	No	No
PING	Yes	Yes (ICMP)	No
INETD	n/a	Yes	No
ROUTED	n/a	Yes	No
SNMP	Yes	Yes	No
BOOTP	Yes	Yes	No
DHCP	Yes	Yes	Client provided by Adapter and Protocol Services
DDNS	Yes	Yes	Client provided by Adapter and Protocol Services
Domain Name System	Yes	Yes	No (DDNS server supercedes IBM TCP/IP V2.0 for OS/2 Domain Name Server Kit)
NFS	Yes	Yes	IBM TCP/IP V2.0 for OS/2 NFS Kit
X Window System	Yes	Yes	IBM TCP/IP V2.0 for OS/2 X Window Server and X Window Client Kits

5.17 Removing TCP/IP Services

If you no longer need TCP/IP Services on your OS/2 Warp Server system, you can use the OS/2 Warp Server Remove folder located in the System Setup folder. The OS/2 Warp Server Remove folder contains an icon representing the ASCII text instructions for removing TCP/IP Services from your OS/2 Warp Server system.

5.18 TCP/IP Related Publications

This section provides the reader with a list of selected publications for further reading on the topics discussed in this chapter. For your convenience, the publications have been grouped by categories.

- TCP/IP for OS/2 documentation, available online with OS/2 Warp Server
  - *TCP/IP for OS/2 - Overview*
  - *Internet Connection for OS/2 - Overview*
  - *Guide to TCP/IP for OS/2*
  - *TCP/IP for OS/2 Command Reference*
  - *Dynamic IP Introduction*
  - *DHCP Administration Guide*
  - *Dynamic DNS Implementation Guide*
  - *DNS Administration Reference*
  - *Ultimedia Mail/2 User's Guide*
  - *Ultimedia Mail/2 Frequently Asked Questions*
  - *DOS/Windows Access Kit*
  - *REXX Sockets API*
  - *REXX FTP API*
- TCP/IP for OS/2 documentation, available as separate publications
  - *Exploring LAN Connectivity with OS/2 Warp Connect*, GG24-4505
  - *TCP/IP 2.0 for OS/2 Installation and Interoperability*, GG24-3531
- Learning about TCP/IP
  - *OS/2 WARP Internet Connection*, SR28-5667, ISBN 1-56884-465-4
  - *Inside TCP/IP*, SR28-5701, ISBN 1-56205-354-X
  - *Internetworking with TCP/IP Vol. I*, SR28-5891, ISBN 0-13-468505-9
  - *The World Wide Web Unleashed*, ISBN 0-672-30737-5
  - *TCP/IP Tutorial and Technical Overview*, GG24-3376
- TCP/IP advanced topics.
  - *Internetworking with TCP/IP Vol. II*, SR28-5892, ISBN 0-13-472242-6
  - *Internetworking with TCP/IP Vol. III*, SR28-5893, ISBN 0-13-474222-2
  - *TCP/IP Network Administration*, SR28-4853, ISBN 0-937175-82-X

Chapter 6. NetBIOS over TCP/IP (TCPBEUI)

This chapter discusses NetBIOS Name resolution issues for the OS/2 Warp Server environment with OS/2 LAN Server, OS/2 LAN Requester and DLS client, as well as the Microsoft Windows 95 or Windows NT client. This chapter assumes the reader has read Chapter 4, "Adapter and Protocol Services" on page 125 and Chapter 5, "TCP/IP Services" on page 167, and is familiar with basic TCP/IP.

6.1 Overview of NetBIOS Name Resolution over TCP/IP Network

Clients and servers need to know how to find one another in order to share information. The NetBIOS conventions built into DOS, and OS/2 clients/servers use 16 byte NetBIOS names which refer to one another by name. Different applications on the same PC uses different names to represent their applications.

NetBIOS names, like *Steve's_PC* or *Printer_HP1* can be built into programs or solicited from humans with relative ease. NetBIOS names can be used as unambiguous identifiers even if a station is moved to another location. However, to send one another packets of information, the TCP/IP protocol drivers of the respective PCs must refer to one another by IP address. The problem exists, then, of having to translate NetBIOS Names into IP addresses in order to effect PC-to-PC communication on an IP network.

To date, this translation has been handled in one of two ways: by use of static tables residing on each client and server, or by use of (dynamic) broadcast queries (packets sent to every client and server) asking in effect *Where is Steve's_PC?*

The problem with static tables is that they must be continually updated and maintained, an activity far more troublesome than the maintenance of IP addresses alone. Every time any new station is added to the network, all of its applications' names must be added to the static table of each other station that wants to send it data. And with static entries, though the name is always mappable, there is no telling whether the named application is actually active at the time interaction is desired by another station. The problem with broadcast queries is that IP networks cannot propagate broadcasts beyond a single (logical) cable segment. Resources located on the other side of a router from the broadcasting station will not receive the query. Every station on the same side of the router will be pestered with queries for which it doesn't know the answer.

A *NetBIOS over TCP/IP* protocol has been defined by the governing TCP/IP standards body, the Internet Engineering Task Force (IETF), which overcomes each of these problems. The IETF standard describes how NetBIOS stations may interact with a NetBIOS Name Server in order to dynamically register their own application names and to learn the name-to-address mappings of other applications.

This chapter describes the existing support level of OS/2 Warp Server, how NetBIOS name resolution is done at the client's side and how to configure a DNS (or DDNS) domain file to have LAN Server names and domain names.

© Copyright IBM Corp. 1996

At the end of this chapter, in section 6.9, "Using NetBIOS Name Server" on page 275, we describe a vendor solution for the full dynamic NetBIOS name resolution.

6.2 NetBIOS over TCP/IP on OS/2 Warp Server

Several components of OS/2 Warp Server can use NetBIOS for communications, but they can also use other protocols like TCP/IP or IPX. File and Print Sharing Services remains the only OS/2 Warp Server component that can only use NetBIOS as a programming interface. As described in Chapter 4, "Adapter and Protocol Services" on page 125, OS/2 requester and DOS LAN Services, and OS/2 LAN Server interface to LM10 NetBIOS API.

The original NetBIOS protocol has some specific characteristics which limit its use in certain wide area network environments:

- The NetBIOS protocol uses a flat name space.
- The NetBIOS protocol relies on the broadcast technique to register/find a name.
- The NetBIOS protocol cannot be routed.

One solution to overcome these limitations can be found in RFCs 1001 and 1002. They describe the standard way to implement the NetBIOS services on top of the TCP and UDP protocols. Adapter and Protocol Services provide a full TCP/IP protocol stack and a TCPBEUI protocol stack, which is a ring 0 implementation of RFC 1001/1002.

Note: In order to use NetBIOS over TCP/IP, you do not need to install the TCP/IP Services of OS/2 Warp Server since the support for this combination of protocols is fully included in Adapter and Protocol Services.

TCP/IP Services of OS/2 Warp Server means TCP/IP applications on top of the TCP/IP protocol, such as FTP, LPR, DHCP and DDNS.

Another solution of routing NetBIOS is to use the NetBIOS over IPX protocol driver which is also supplied with Adapter and Protocol Services.

The capability of running NetBIOS applications over routable protocols offers new flexibility when designing OS/2 Warp Server networks. OS/2 Warp Server systems, Warp Connect Peer workstations, LAN Servers, and LAN Requester workstations can be on remote LAN segments connected by IP routers. This also means that such systems can be introduced into existing TCP/IP networks without introducing an additional network protocol (NetBIOS).

There are several defined classes of NetBIOS over TCP/IP implementations specified by RFCs 1001 and 1002. The simplest, and the one most widely implemented, is the Broadcast Node (B-node) implementation. This covers TCP/IP-implemented environments which support broadcast and Ethernet in particular. The point-to-point node (P-node) implementation operates in environments where NetBIOS Name Server (NBNS) is available as defined in the RFC 1001/1002. The mixed node (M-node) is now called H-node and it operates P-node but if NetBIOS Name Server is not available or it cannot resolve a name, it operates like B-node.

OS/2 TCPBEUI is a high performance, ring 0, implementation of NetBIOS over TCP/IP. TCPBEUI provides the LM10 protocol driver interface. It is the same LM10 functionality that is also provided by NetBEUI. Figure 186 on page 261 shows this interface. TCPBEUI maps NetBIOS API calls into the TCP/IP protocol. NetBIOS over TCP/IP contains enhancements over the B-node standard which improve system performance by decreasing broadcast frames and by expanding communications over routers and bridges. These enhancements, described in 6.4, "Reducing Broadcast Frames with TCPBEUI" on page 264, are transparent to NetBIOS applications and do not interfere with other B-node implementations that lack similar functions.

RFC 1001/1002 is not an encapsulation technique, but rather builds special packets and sends them out via UDP and TCP. For example, once a NetBIOS session has been established, TCPBEUI will use sockets-send commands over a TCP connection to send NetBIOS session data. TCPBEUI builds a four-byte session header that precedes the actual user data. Thus, a NetBIOS Chain Send of 128KB would have an overhead of only four bytes.

TCPBEUI allows peer-to-peer communication over the TCP/IP network with other computers which have compatible services. Figure 186 shows the relationship between the NetBIOS, NetBIOS over TCP/IP, and TCP/IP protocol stacks as implemented in Adapter and Protocol Services.

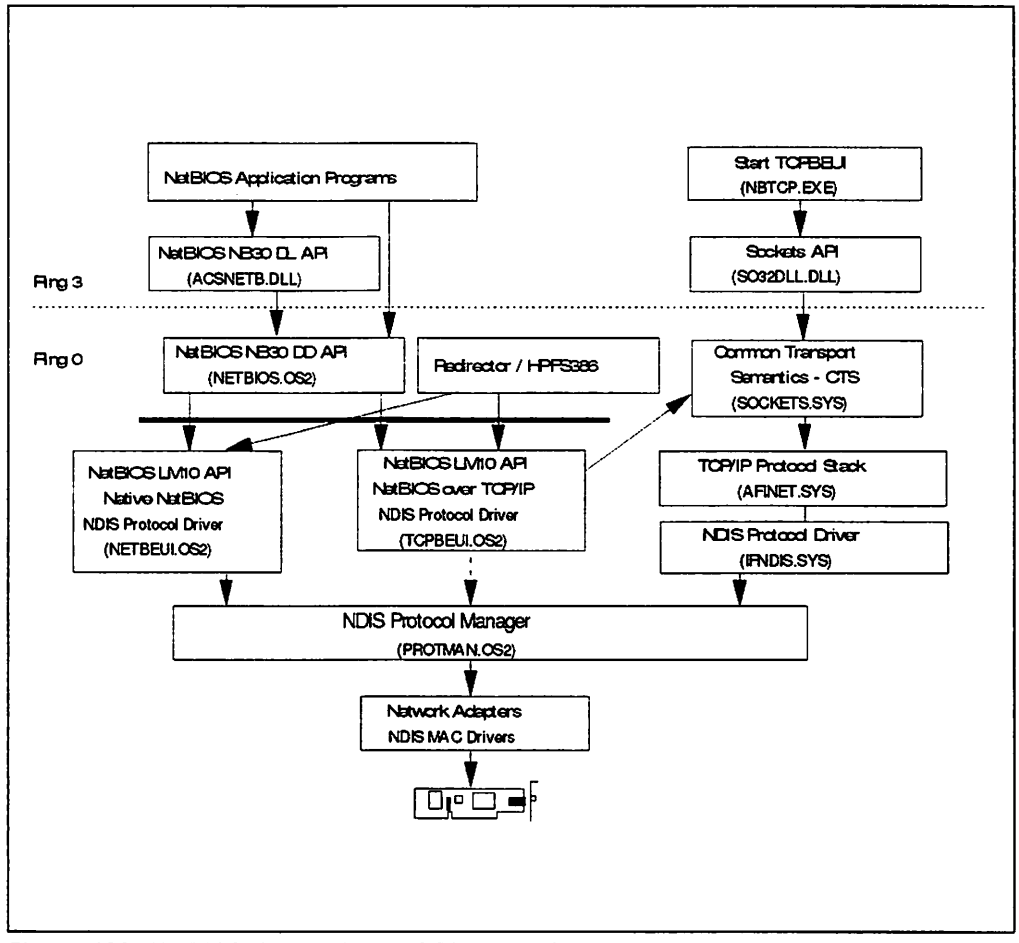


Figure 186. NetBIOS, NetBIOS over TCP/IP and TCP/IP Structure

Unlike NETBEUI.OS2, the TCPBEUI.OS2 program doesn't directly communicate with the NDIS interface. The dotted line in the figure indicates TCPBEUI has a

BINDINGS statement in the PROTOCOL.INI file but a bind process is only required in order to create a control block area.

Figure 186 on page 261 also illustrates how NetBIOS applications can use both NETBEUI and TCPBEUI protocol stacks. ACSNETB.DLL provides the ring 3 NetBIOS DLL API for application programs. Ring 3 NetBIOS commands are sent to NETBIOS.OS2 for processing. NETBIOS.OS2 provides the ring 0 NetBIOS DLL API for applications and other device drivers to use, and it binds to one or more LM10 (LAN Manager 1.0) transport protocol drivers.

The LAN redirector component of File and Print Sharing Services (NETWKSTA.200), and HPFS386 uses the LM10 interface.

Support for NetBIOS over TCP/IP can easily be added to the existing NetBIOS structure since the Warp Server Install program supports up to four LM10 interfaces. It is provided by having NETBIOS.OS2 bind to TCPBEUI.OS2. To enable NETWKSTA.200 to use TCPBEUI, there must be a `NETx` (where x is 1, 2, 3, 4, for example) statement in the IBMLAN.INI file configured appropriately (see Figure 189 on page 264).

Data transfer to LAN is handled by a MAC device driver, for example the IBMTOK.OS2 device driver.

6.3 TCPBEUI Coexistence with NetBEUI

Adapter and Protocol Services provide the capability of configuring NetBIOS applications, especially File and Print Sharing Services, with both NetBEUI and TCPBEUI on the same network interface card. This dual protocol stack configuration will allow local sessions to continue running with NetBEUI performance while also providing wide area network connectivity with NetBIOS over TCP/IP.

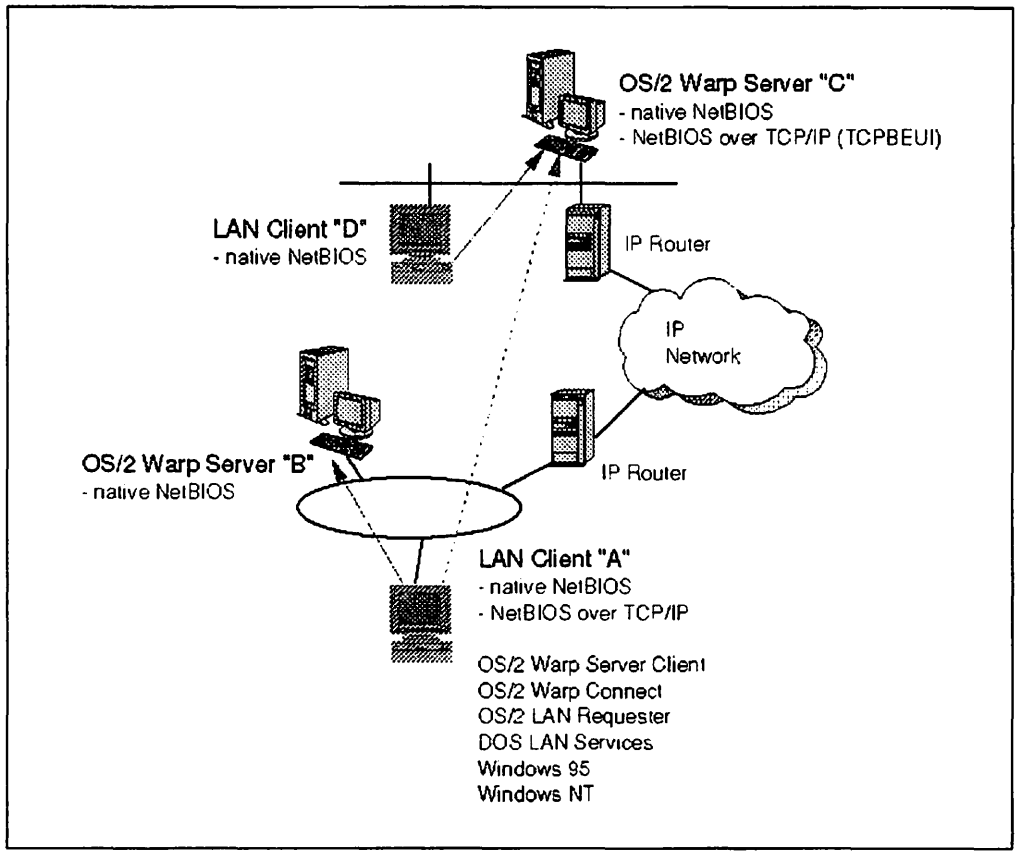


Figure 187. TCPBEUI Coexistence

Figure 187 shows an example scenario with both TCP/IP and NetBIOS protocols being used and TCP/IP Services installed on a server. In this example, LAN Client A is able to access File and Print Sharing Services resources on the OS/2 Warp Server B on the local LAN segment via NetBIOS, and the OS/2 Warp Server C on the remote LAN segment across the IP network via TCPBEUI. In addition, it is able to use the TCP/IP applications provided by TCP/IP Services to access local and remote TCP/IP hosts via the native TCP/IP protocol.

Adapter and Protocol Services provide the TCP/IP protocol capability with or without TCP/IP Services installed, but with only a limited set of TCP/IP functions and services. These functions basically enable you to configure IP interfaces and routes and to test the TCP/IP protocol for proper operation:

- ARP
- HOST
- HOSTNAME
- IFCONFIG
- IPTRACE
- IPFORMAT
- NETSTAT
- PING
- ROUTE

When configuring Adapter and Protocol Services for both NetBEUI and TCPBEUI, even though a single LAN adapter is present in the workstation, the two protocols need to be configured on different logical adapters. The Current Configuration window on the LAPS Configuration panel should be changed as follows:

```
IBM Token-Ring Network Adapter ...
  0  - IBM OS/2 NETBIOS
  0  - IBM IEEE 802.2
  0  - IBM TCP/IP
  1  - IBM OS/2 NETBIOS OVER TCP/IP
```

Figure 188. LAPS Configuration Panel. Single Token-Ring Adapter bound to NetBIOS, IEEE 802.2 and TCPBEUI

Note that the logical numbers of the protocol drivers must be set differently although only one physical LAN adapter is present.

File and Print Sharing Services handle this configuration as if there were two adapters present. Therefore, two NET entries will be made in IBMLAN.INI file:

```
[networks]

net1 = NETBEUI$,0,LM10,102,175,14
net2 = TCPBEUI$,1,LM10,102,175,14

[requester]

wrknets = NET1,NET2

[server] srvnets = NET1,NET2
```

Figure 189. IBMLAN.INI for Two NetBIOS Networks. NetBIOS and TCPBEUI bound to a single LAN adapter (Extract).

6.4 Reducing Broadcast Frames with TCPBEUI

NetBIOS over TCP/IP, or TCPBEUI, provides an extension to B-node. It is called *Routing Extensions*. The purposes of the routing extensions are to enable a communication over different subnets, and to reduce broadcast traffics. This section discusses these topics and also gives you information on how to use an existing Domain Nameserver (DNS) in a TCPBEUI environment. With all these settings, you can reduce TCP/IP broadcast frames on the network.

Routing Extensions

Three of the enhancements to TCPBEUI are in the form of *routing extensions*. These extensions allow communication between networks and over IP routers and bridges. The routing extensions are:

Names File

A names file consists of pairs of a NetBIOS name and an IP address. NetBIOS over TCP/IP will conduct a prefix search of the names file before broadcasting on the network. The prefix match succeeds if the entry in the names file matches the given name, up to the length of the entry. The first match is used; therefore, the order in which NetBIOS names are listed in the names file is important.

To enable this routing extension, set the NAMESFILE parameter in the TCPBEUI section of PROTOCOL.INI to a nonzero integer that represents the number of names file entries.

Domain Nameserver (DNS)

A network administrator can maintain pairs of NetBIOS names and IP addresses in a DNS. If a name query fails, NetBIOS over TCP/IP can append the NetBIOS Domain Scope String to the encoded NetBIOS name and issue a request to the DNS to look up an IP address for that NetBIOS name. The Domain Scope String is defined by the PROTOCOL.INI parameter `DOMAINSCOPE`.

For more information on how to set up the DNS with the NetBIOS names, see "Storing NetBIOS Names on the Domain Nameserver" on page 266.

Broadcast File

A broadcast file contains a list of host names, host addresses or directed broadcast addresses. It is read at startup, and each valid address is added to the set of destination addresses for broadcast packets. Remote nodes included in the broadcast file are then treated as if they were on the local network. Use of a broadcast file has the effect of extending a node's broadcast domain to its own subnet and to any other subnets listed in the broadcast file. A maximum of 32 broadcast file entries are supported, each of which could include additional subnets, thus extending the node's broadcast domain.

If your routers support directed broadcasts (that is, you can ping the broadcast address of a distant IP subnet, and get back a response from all the stations on that subnet), then you can place the broadcast address for each subnet in the server's broadcast file. Also enable the TCPBEUI name cache described in "Name Cache and Name Discovery Algorithm" on page 266. This greatly reduces broadcast traffic and eases administration. (The clients still need to know the IP address and NetBIOS name of each server and peer server.)

Configuring TCPBEUI Routing Extensions

Use the LAPS configuration program (which is shown in Figure 101 on page 143) and add the IBM OS/2 NetBIOS over TCP/IP protocol to an adapter. Then double-click on **IBM OS/2 NetBIOS over TCP/IP** to invoke the following menu:

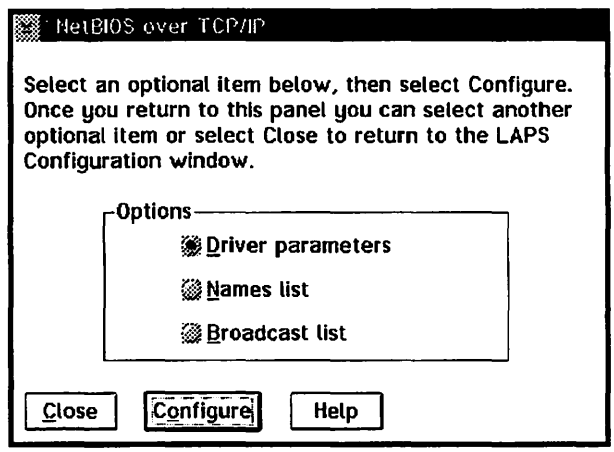

NetBIOS over TCP/IP
Select an optional item below, then select Configure. Once you return to this panel you can select another optional item or select Close to return to the LAPS Configuration window.
Options
Driver parameters
Names list
Broadcast list
Close
Configure
Help

Figure 190. TCPBEUI Configuration

On this menu, select:

Driver parameters to configure the parameters for the TCPBEUI protocol.

Names list to configure the names file (\IBMCOM\RFCNAMES.LST).

Broadcast list to configure the broadcast file (\IBMCOM\RFCBCST.LST).

When you make changes to the names or broadcast files while TCPBEUI is active, you can reinitialize TCPBEUI with the new files using the RFCADDR.EXE program.

Name Cache and Name Discovery Algorithm

Another enhancement NetBIOS over TCP/IP provides is a *name cache* for storing remote names that have been discovered. Since TCPBEUI uses broadcasting as a mechanism for name discovery, by checking the cache first, broadcast traffic can be reduced. This cache is enabled by setting the NAMECACHE parameter in the TCPBEUI section of the PROTOCOL.INI to a nonzero integer that represents the number of names stored in the directory.

The information in the remote name cache (or directory) is also stored on disk (in the \IBMCOM\RFCCACHE.LST file) and periodically updated. When the system is restarted, this information can be preloaded into the cache at bootup time. Preloading can reduce the amount of broadcast frames on the network since NetBIOS will not have to rediscover names for remote workstations. To preload the remote names cache, set the `PRELOADCACHE = YES` in the TCPBEUI section of the PROTOCOL.INI file.

When NetBIOS over TCP/IP is searching for a name, the following name discovery algorithm is used:

1. Check the local name cache first.
2. If not found, check the local names file.
3. Next, issue GetHostByName() to the Domain Nameserver. The tcpip\etc\hosts file is checked if the GetHostByName to the DNS fails.
4. Finally, issue a broadcast using the broadcast file's entries.

It is recommended that when running NetBIOS over TCP/IP in a wide area network (WAN), you should turn name caching on at the server (for instance, setting it to a value of 100).

Storing NetBIOS Names on the Domain Nameserver

In a larger network where a DNS already exists, you can use the DNS database to store NetBIOS names and IP addresses pairs, thereby eliminating the need for maintaining a broadcast file or names file on each client. In each client PROTOCOL.INI file, you must only ensure that the DOMAINSCOPE parameter is set to the TCP/IP domain name. TCPBEUI will then know to search that domain's DNS for the IP address of the requested server.

Notes:

1. The solution described in this section assumes that the server is already set up as a TCP/IP machine with a host name/IP address pair that is registered in the DNS database.
2. If you do not have a DNS, you can set up the local node's hosts file (\tcpip\etc\hosts) in the same way we describe here. That is, the NetBIOS names must be encoded in the hosts file just as they must be in the DNS. TCPBEUI will first look for the requested server IP address in the DNS; if one does not exist or the address is not specified in the DNS, TCPBEUI checks for the local hosts file.

The servers' NetBIOS names must be added to the DNS database in an *encoded* format. The encoding is necessary because NetBIOS names are 16 bytes of *any* bit pattern, and a TCP/IP DNS only accepts host names in the character set *A to Z* and *0 to 9*.

For example, if you have specified

```
DOMAINSCOPE=austin.ibm.com
```

in the PROTOCOL.INI file and the NetBIOS name you have requested is not found in the local names cache or the local names file, then a sockets GetHostByName(netbios_name.austin.ibm.com) call will be made. TCPBEUI translates the 16-byte NetBIOS name into a 32-byte reversible, half-ASCII biased encoded format, such as:

```
GetHostByName(GCHCGJGDGFCACACACACACACACACACA.austin.ibm.com)
```

and sends it to the DNS. If the DNS knows this name, it sends back the IP address to TCPBEUI. For this to work, the administrator must store the NetBIOS names in the DNS in the encoded format.

How do you encode NetBIOS names and store them in the DNS database? You must encode the 16 byte name into a 32-byte string using the MAPNAME utility, which is located in the APPLETS directory of MPTS diskette 5 (MPTSAPLT.ZIP). This file can also be found on the OS/2 Warp Server CD-ROM under the \CID\SERVER\IBMLS\IBM500N5 subdirectory. Then, you store the names in the DNS database so that they point back to the original host name, where the TCP/IP address is already listed. We will take you through an example of how to do this.

For each server, there will be at least three entries in the DNS database in addition to the initial host name entry. (Remember, we are assuming that the LAN Server is already set up as a TCP/IP host with a host name/IP address pair that is registered in the DNS database.) The three entries are necessary because LAN Server issues a NetBIOS NCB.AddName call three times, using the computername specified in the IBMLAN.INI file and ending each with a unique hex value as the sixteenth byte. The hex values used as the sixteenth byte are 0x20 (blank or null), 0x00 and 0x03. If the server is a domain controller, there must be a fourth entry, the encoded domain name with the sixteenth byte of 0x00.

Let's say that we have a DNS already set up on our network. We have installed LAN Server 4.0 on the domain controller and one additional server. Both machines also have TCP/IP for OS/2 installed, and their host names are registered in the DNS database. We want to configure for TCPBEUI so that clients can access servers across our IP router without requiring a broadcast file or names file at each client. To do this, we will take advantage of the DNS, and add the appropriate DOMAINSCOPE entry to each client's PROTOCOL.INI file.

In this example, our domain name is ITSCAUS, and our two servers are configured as follows:

Domain controller Computername: ITSCSV00
TCP/IP host name: ITSCWK00

Additional server Computername: ITSCSV01
TCP/IP host name: ITSCWK01

Note: The computername refers to the IBMLAN.INI parameter. This is also referred to as the server name or machine ID.

Here's an extract from our DNS database *before* we add the encoded NetBIOS names:

```
ITSCWK00                        86400  IN  A      129.35.144.210
                                       IN  HINFO  DC HOST NAME
;
ITSCWK01                        86400  IN  A      129.35.144.211
                                       IN  HINFO  AS HOST NAME
;
```

Figure 191. Sample DNS Database File Before Adding Encoded NetBIOS Names. The TCP/IP host names are listed with the workstation IP addresses.

The HINFO keyword specifies comment information. In this case, we have indicated that ITSCWK00 is the TCP/IP host name for the domain controller, and ITSCWK01 is the host name for the additional server. TCP/IP looks up the host name in the DNS database and finds the actual IP address.

Now we want to use TCPBEUI and take advantage of the DNS database. To do this, we must encode the server NetBIOS names using the MAPNAME utility. Typing MAPNAME by itself will give you help on how to use the command. The utility converts NetBIOS names to RFC-encoded names and vice versa. Using our example, the following steps show you how to encode your server NetBIOS names.

MAPNAME Requires Uppercase NetBIOS Names

When using MAPNAME, be sure to type any NetBIOS names in *uppercase* letters, as this is a case-sensitive utility. If you type names in lowercase, the output will be incorrect.

1. Use the MAPNAME utilty with the /RB parameters to specify that you want the output to be in RFC format and padded with blanks for up to 16 characters.

   ```
   MAPNAME ITSCSV00 /RB
   ```

   The following 32-byte encoded name is displayed:

   ```
   RFC name: EJFEFDEDFDFGDADACACACACACACACACA
   ```

   This is the first of the four encoded names you need for the domain controller. Here, the sixteenth byte, CA, is null (0x20). The following command would have given us the same result, but since null characters are the default, the L20 is unnecessary.

   ```
   MAPNAME ITSCSV00 /RBL20
   ```

2. This time, also use the L parameter to specify that you want the last character of the output to be 0x00, as follows:

   ```
   MAPNAME ITSCSV00 /RBL00
   ```

   The result is:

   ```
   RFC name: EJFEFDEDFDFGDADACACACACACACACAAA
   ```

   AA is hex 0x00.

3. Again, use the L parameter to specify the last character of the output to be 0x03, as follows:

   ```
   MAPNAME ITSCSV00 /RBL03
   ```

You receive this output:

```
RFC name: EJFEFDEDFDFGDADACACACACACACAAD
```

AD is hex 0x03.

4. Because this is the domain controller, you must also specify the encoded domain name with the sixteenth byte of 0x00, as follows:

   ```
   MAPNAME ITSCAUS /RBL00
   ```

   The encoded name is:

   ```
   RFC name: EJFEFDEDFDFGDADACACACACACACAAA
   ```

5. Now we go through the first three steps for the additional server, ITSCSV01, to get the following output (Do not encode the domain name for additional servers):

   ```
   MAPNAME ITSCSV01 /RB
   RFC name: EJFEFDEDFDFGDADBCACACACACACACACA

   MAPNAME ITSCSV01 /RBL00
   RFC name: EJFEFDEDFDFGDADBCACACACACACACAAA

   MAPNAME ITSCSV01 /RBL03
   RFC name: EJFEFDEDFDFGDADBCACACACACACACAAD
   ```

6. Edit the DNS database to add the entries for the domain controller and additional server. Use the DNS CNAME keyword to point back to the host name entry for the machine where the actual IP address is already specified. In other words, the encoded names we have generated are *aliases* for the host names ITSCWK00 and ITSCWK01.

   Note: You cannot have two entries pointing to the same IP address; so you must use the CNAME keyword to create aliases.

   The following example shows how our DNS database file looks *after* adding the NetBIOS encoded names. Again, we use HINFO to designate comments.

```
ITSCWK00                          86400  IN  A      129.35.144.210
                                         IN  HINFO  DC HOST NAME
;
EJFEFDEDFDFGDADACACACACACACACACA 86400  IN  CNAME  ITSCWK00
                                         IN  HINFO  ITSCSV00 (0x20 in byte 16)
;
EJFEFDEDFDFGDADACACACACACACACAAA 86400  IN  CNAME  ITSCWK00
                                         IN  HINFO  ITSCSV00 (0x00 in byte 16)
;
EJFEFDEDFDFGDADACACACACACACACAAD 86400  IN  CNAME  ITSCWK00
                                         IN  HINFO  ITSCSV00 (0x03 in byte 16)
;
EJFEFDEDFDFGDADACACACACACACACAAA 86400  IN  CNAME  ITSCWK00
                                         IN  HINFO  ITSCAUS (0x00 in byte 16)
;
ITSCWK01                          86400  IN  A      129.35.144.211
                                         IN  HINFO  AS HOST NAME
;
EJFEFDEDFDFGDADBCACACACACACACACA 86400  IN  CNAME  ITSCWK01
                                         IN  HINFO  ITSCSV01 (0x20 in byte 16)
;
EJFEFDEDFDFGDADBCACACACACACACAAA 86400  IN  CNAME  ITSCWK01
                                         IN  HINFO  ITSCSV01 (0x00 in byte 16)
;
EJFEFDEDFDFGDADBCACACACACACACAAD 86400  IN  CNAME  ITSCWK01
                                         IN  HINFO  ITSCSV01 (0x03 in byte 16)
;
```

Figure 192. Sample DNS Database File After Adding Encoded NetBIOS Names. The encoded NetBIOS names point back to the TCP/IP host names (using CNAME), where the workstation IP addresses are specified.

For the domain controller (ITSCSV00), there are four encoded entries, three for the server name (computername) and one for the domain name (ITSCAUS). For the additional server (ITSCSV01), there are three encoded entries for the server name. The encoded entries are all aliases that point back to the host names.

7. On your clients, be sure that you set the DOMAINSCOPE parameter to point to the correct TCP/IP domain, for example:

   ```
   DOMAINSCOPE=austin.ibm.com
   ```

   This enables TCPBEUI to use the DNS to find the NetBIOS name/IP address pairs, eliminating the need for a broadcast file or names file at each client.

Notes:

1. It does not make any difference if you are using an existing DNS server, or if you are using a new dynamic DNS server which is a part of TCP/IP Services of OS/2 Warp Server. Since the dynamic DNS server cannot determine the difference between a TCP/IP host name and an RFC-encoded NetBIOS name, you still have to add those resource records manually.
2. The RFCs 1001/1002 also specify a NetBIOS name server and NetBIOS datagram distribution server functions. Apart from returning IP addresses when queried with NetBIOS names, those servers would also allow clients to register, update and delete their NetBIOS names and IP addresses with the server dynamically. RFC NetBIOS servers would also take care of proper NetBIOS datagram delivery throughout a TCP/IP network. Such functions are not implemented in OS/2 Warp Server.

For further information on the Domain Name Server, please refer to the *DNS Administration Reference* and *Dynamic DNS Implementation Guide*, available as

online books with OS/2 Warp Server. They are located in the DDNS Server Services folder inside the TCP/IP folder.

6.5 Configuring TCPBEUI to Support 1000 Clients

The new TCPBEUI protocol driver that is included in OS/2 Warp Server can be bound to one adapter up to four times, thus providing the capability to support 1000 client workstations by using the NetBIOS over TCP/IP protocol. The following should be considered before setting up this kind of configuration:

1. One adapter with four TCPBEUIs

   This is the only method possible to provide TCPBEUI support for 1000 clients. This is because TCPBEUI can only be used with the lan0 TCP/IP interface. The obvious question is not performance but the single point of failure in this configuration.

2. Four adapters on different IP subnets

   This configuration will allow you to start the server or requester without any errors, but no clients or peers can connect from any IP subnets other than the one used with the lan0 interface. This configuration is therefore neither recommended nor supported.

3. Four adapters on the same IP subnet

   This configuration is not possible since TCPBEUI will detect a NetBIOS name conflict. This configuration is therefore neither recommended nor supported.

Figure 193 on page 272 illustrates how TCPBEUI can be used four times over a single LAN adapter in order to support 1000 NetBIOS clients from a single OS/2 Warp Server system.

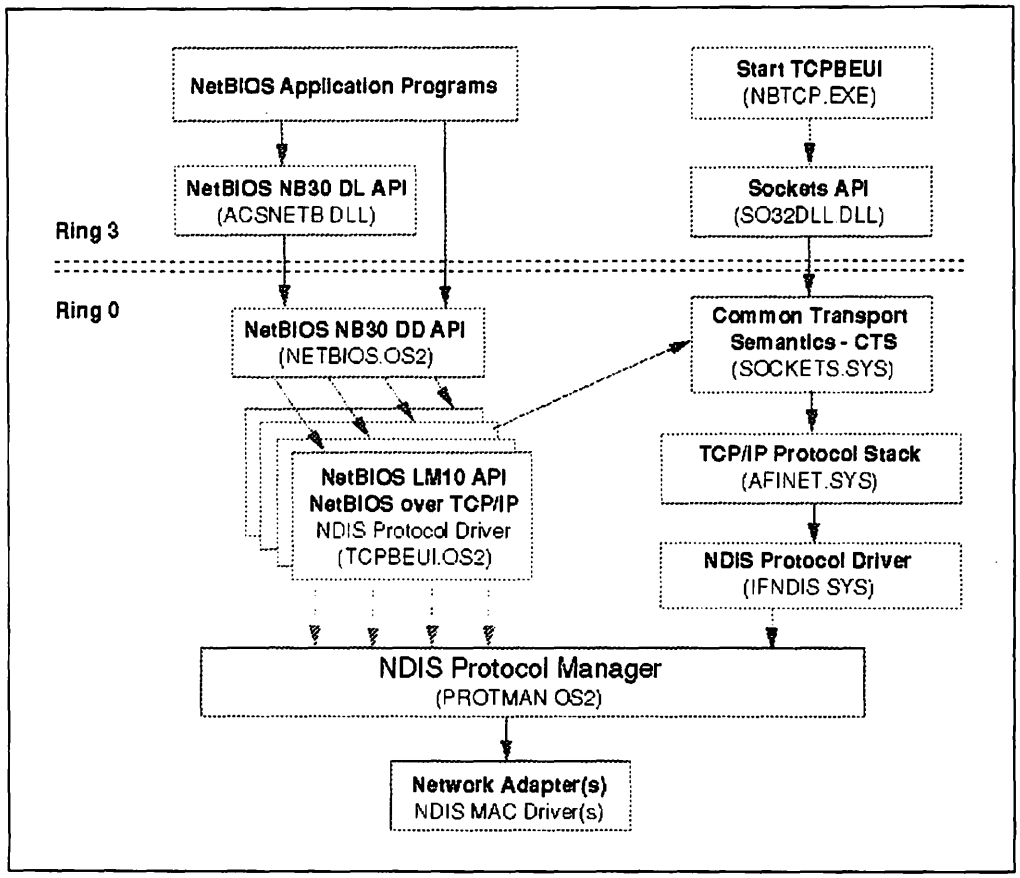


Figure 193. TCPBEUI Configuration for 1000 Clients

The following lines are extracted from the PROTOCOL.INI file to reflect what drivers must be loaded in order to support the configuration as shown above:

```
...

[NETBIOS]

   DriverName = netbios$
   ADAPTER0 = tcpbeui$,0
   ADAPTER1 = tcpbeui$,1
   ADAPTER2 = tcpbeui$,2
   ADAPTER3 = tcpbeui$,3

[tcpbeui_nif]

   DriverName = tcpbeui$
   Bindings = IBMTOK_nif,IBMTOK_nif,IBMTOK_nif,IBMTOK_nif
   OS2TRACEMASK = 0x0
   SESSIONS = 130
   NCBS = 225
   NAMES = 21
   SELECTORS = 15
   USEMAXDATAGRAM = "NO"
   NETBIOSTIMEOUT = 500
   NETBIOSRETRIES = 2
   NAMECACHE = 100
   PRELOADCACHE = "YES"
   NAMESFILE = 50
   DATAGRAMPACKETS = 20
   PACKETS = 150

[tcpip_nif]

   DriverName = TCPIP$
   Bindings = IBMTOK_nif

[IBMTOK_nif]

   DriverName = IBMTOK$
   MAXTRANSMITS = 6
```

```
RECVBUFS = 2
RECVBUFSIZE = 256
XMITBUFS = 2
XMITBUFSIZE = 4224
```

6.6 Using TCPBEUI with Dial-Up Connections

The purpose of NetBIOS over TCP/IP is to allow applications to use the NetBIOS protocol in a wide area network (WAN). So far, we have discussed the usage of TCPBEUI in LAN configurations only. This would have implied that a router must be available somewhere in order to actually access the TCP/IP WAN. What if the gateway to the WAN should be the OS/2 Warp Server itself, and the remote client does not have any LAN attachment? The following points should be considered for that kind of configuration:

1. As we have seen before, TCPBEUI will only work with the lan0 TCP/IP interface.
2. Since TCPBEUI is implemented as an NDIS protocol driver, it must be bound to an adapter driver in PROTOCOL.INI.
3. There is no NDIS loopback MAC driver supplied with OS/2 Warp Server in order to fake a lan0 interface for TCP/IP and TCPBEUI.

Therefore, a dial-up connection for TCPBEUI will only work if a physical LAN connection exists for the systems on either end of the WAN link. Hence, we recommend using Remote Access Services in this case.

6.7 Performance Considerations for TCPBEUI

The performance when using TCPBEUI is generally slower than using native NetBIOS due to the additional overhead of mapping NetBIOS API calls to TCP/IP. (However, using OS/2 Warp Server over TCPBEUI is significantly faster than using LAN Server 3.0 with the TCP/IP 2.0 NetBIOS kit because there is no longer a transition overhead from ring 3 to ring 0.) The performance difference can range widely depending on the environment. Some environmental factors that can affect performance are the type of client (OS/2 or DOS), the server CPU workload, the type of network operations being performed, the network media, network congestion, and communication line speeds. We've observed the performance of NetBIOS over TCP/IP being anywhere from 10 percent slower to as much as four times slower than NetBEUI.

One of the environments in which performance tests were conducted was a medium-sized LAN on 16Mbps token ring with no WAN connections. We ran a set of industry standard business applications on TCPBEUI clients and again on OS/2 NetBEUI clients. In this environment, NetBIOS over TCP/IP was 20 percent slower than NetBEUI. The performance of DOS NetBIOS over TCP/IP clients was significantly less than that of the OS/2 clients.

Database applications generally use small records when accessing shared databases residing on the server. Often these small records are retrieved from the file system cache with no physical disk access being required. The performance of this type of application on NetBIOS over TCP/IP may be noticeably slower than if the application were run using NetBEUI. However, if the number of database accesses of this type in performing a typical operation is in the order of hundreds, not thousands, the user may not notice a difference in performance in the two protocols.

It may be necessary to periodically update client applications or other files by copying them from the server disk. DCDB replication from a domain controller to a remote additional server also generates I/O operations, sometimes known as file transfers. This type of file I/O activity over a network will show little or no performance difference between NetBEUI and TCPBEUI due to protocol characteristics. One should be aware, however, that most WAN connections today are made over relatively low-speed communication lines when compared with a LAN speed of 4 to 16Mbps. File transfer operations over WAN communication lines will probably be slower than over LANs but most likely not due to the network protocol.

Tuning Considerations for TCPBEUI

If you're using NetBIOS over TCP/IP in a token-ring environment, file transfer performance might be improved by increasing the maximum transmissible unit (MTU) size. We have seen up to a 20 percent increase in performance of large file transfers by using an 8KB packet instead of the default 1500 bytes. The default of 1500 was chosen because of Ethernet's packet size limitation and prevalence in TCP/IP environments. The MTU size can be changed with the IFCONFIG command in the \MPTN\BIN\SETUP.CMD file.

Set the MTU size to the desired packet size plus 40 bytes, the maximum TCP/IP header size. The desired packet size should be a multiple of 2048. Your network adapter must be configured to support transmission of buffers that are at least the size specified for the MTU. On an IBM 16/4 Token-Ring Adapter, this would be accomplished by setting the XMITBUFSIZE parameter in the token-ring section of the PROTOCOL.INI file.

Note: If you use LAN adapter cards that need a system memory area below 1MB to map buffer space (memory-mapped I/O), make sure the adapter RAM is set to at least 16KB before you increase the XMITBUFSIZE and MTU size parameters.

Check your network interface card documentation for information on configuring your adapter.

It is also recommended that you use the INETCFG program to change the default keepalive value from the default of 120 minutes to a lower value. The example of the command input is:

```
inetcfg keepalive=3
```

The reason for this is that a TCPBEUI server is *not* informed of a TCP/IP connection breaking for a period of two hours. Thus, a TCPBEUI server could accumulate a large number of *ghost* sessions. By issuing the `inetcfg keepalive=3` command, TCP/IP will inform TCPBEUI after 3 minutes that a TCP/IP connection is broken (that is, a remote client has gone down).

If you are experiencing difficulties accessing a remote server over a slow WAN connection, try gradually increasing the NETBIOSTIMEOUT parameter in PROTOCOL.INI.

When using both NetBEUI (for LAN access) and TCPBEUI (for WAN access), it is best to have both `net1=NETBEUI$` and `net2=TCPBEUI$`, as shown in Figure 189 on page 264. In this dual protocol environment, it is recommended that you decrease NETBIOSRETRIES to 2 or 3 (from the current default of 8). Also, be aware that if the NETBIOSTIMEOUT parameter is set too high, some local LAN functions, such as logon or NET USE command, may take significantly longer.

When TCPBEUI is configured for more than 250 sessions, it is recommended to increase the value of the PACKETS parameter to 150.

Recommendation - Dual Protocol Stack

Because there may be a performance difference in a particular environment, it is recommended to configure and use NetBEUI in the local area network (LAN) environment, and NetBIOS over TCP/IP in the wide area network (WAN) environment. The Adapter and Protocol Services shipped OS/2 Warp Server provide the capability of configuring your server with both NetBEUI and TCPBEUI on the same network interface card.

The dual protocol stack can be configured through the installation/configuration program. When selecting protocols, install logical adapter 0 with NetBEUI and logical adapter 1 with TCP/IP and NetBIOS over TCP/IP (on the same physical adapter). This dual protocol stack configuration allows local sessions to continue running with NetBEUI performance while also providing WAN connectivity with TCPBEUI.

6.8 Removing TCPBEUI Configuration

When removing the TCPBEUI configuration from MPTS, you must first remove TCP/IP Socket Access at the Configure panel (see Figure 100 on page 142), before proceeding to the LAPS Configuration panel and removing the TCP/IP protocol and the NetBIOS over TCP/IP protocol.

If the removal is not performed in this manner, the protocols will be removed from the PROTOCOL.INI file, but the MPTCONFG.INI file will not be updated properly. This will result in invalid device drivers being added to the CONFIG.SYS file.

6.9 Using NetBIOS Name Server

In the market, there are several vendor products which support robust implementation of the RFC 1001/1002 standard, NetBIOS Name Server (NBNS). One example, we tested with, is the Network TeleSystems (NTS) product called Shadow. For information on NTS itself and the product Shadow, open the Web home page of `http://www.ntsi.com`.

NTS product Shadow implements most of RFC 1001/1002 functions such as:

- NetBIOS Name Server function
- NetBIOS Datagram Distributor function

To be able to use any NetBIOS Name Server, OS/2 Warp Server requires a CSD for TCPBEUI.OS2 and TCPBEUI.NIF.

TCPBEUI CSD for H-Node Support

CSD is planned for TCPBEUI H-Node support.

Figure 194 on page 276 illustrates how NetBIOS Name Server works for server and clients over TCP/IP network.

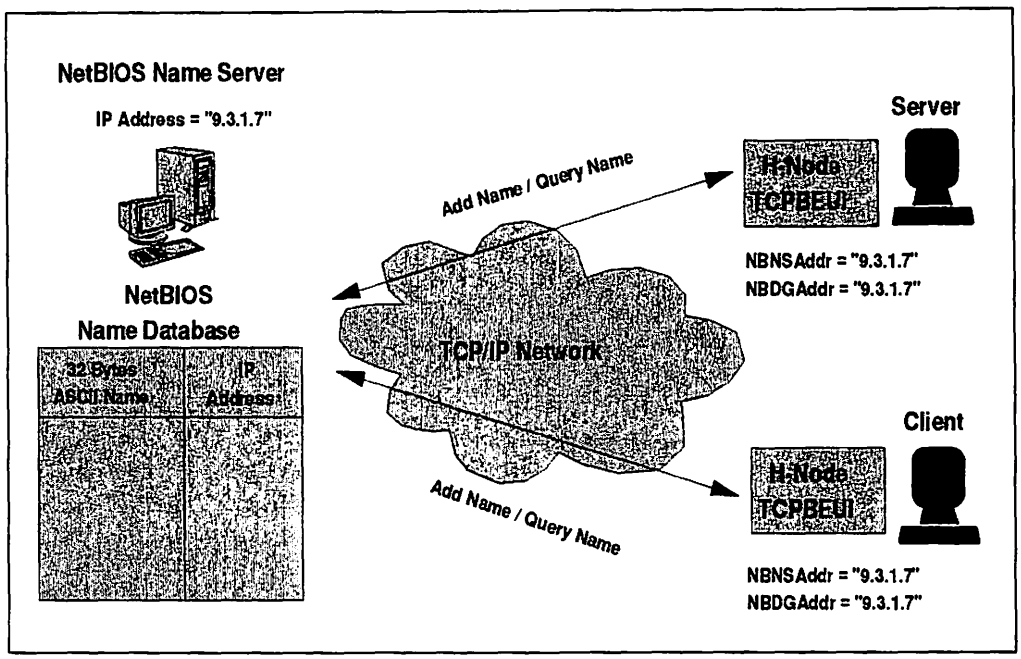


Figure 194. How Server and Client Work with NetBIOS Name Server

In Figure 194, the server registers its domain name (NetBIOS group name) and server name (unique NetBIOS name) to the NetBIOS Name Server (NBNS here after). OS/2 TCPBEUI should have H-node support and PROTOCOL.INI should have a pointer to NBNS, which is the IP address 9.3.1.7 in the figure. The OS/2 client should have the same TCPBEUI code and PROTOCOL.INI file. When the OS/2 requester starts, it registers the requester name to NBNS.

When a user logs on from the client, it must find an IP address of the server. The requester queries NBNS with the target domain name and NBNS returns the server's IP address by looking up its database. Then the requester establishes the session with the server through the TCP/IP network. Figure 195 on page 277 shows the NetBIOS name registration and query process. All of these operations can be done through different subnets, and without any broadcast operation.

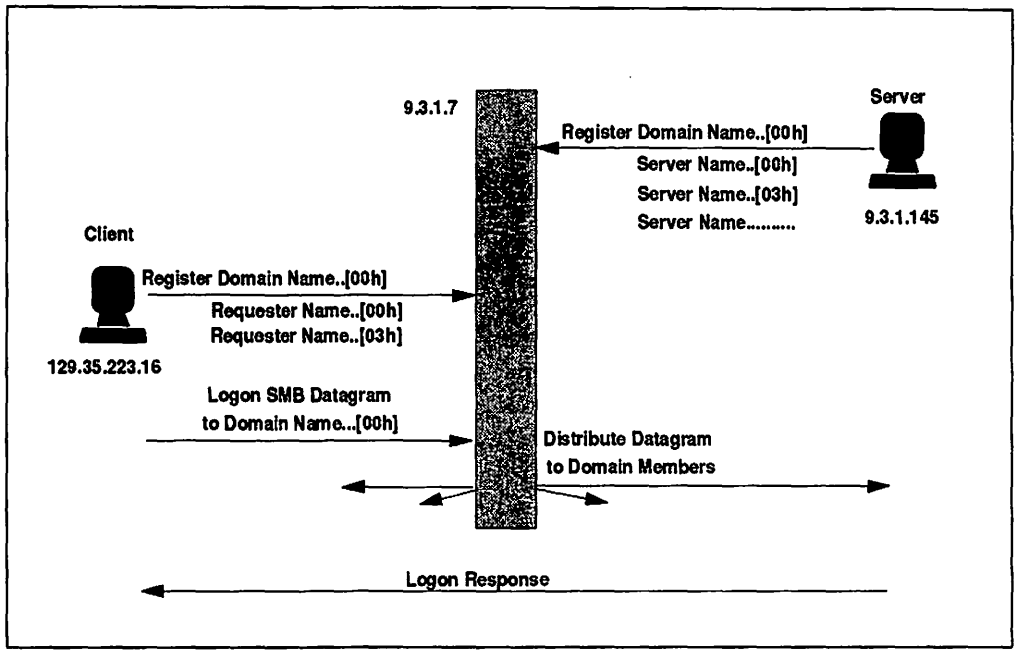


Figure 195. Detail Flow of Server/Client to NetBIOS Name Server

When an SMB datagram is sent from a client to a real NetBIOS local network, it is a datagram to a group name. It means there might be more than one member in a group. Requesters are the members if `DOMAIN =` parameter in the IBMLAN.INI file has the same domain name. More important domain members are additional servers and backup domain controllers. In a real NetBIOS network, backup domain controllers will receive the same logon SMB datagram, so in case the primary domain controller is down the backup will respond to process the logon.

In the TCP/IP network this process is defined as a datagram distributor. Without a datagram distributor function on the network, NetBIOS over TCP/IP has less function than a real NetBIOS network. With this datagram distributor function of NBNS, we can have a backup domain controller somewhere in the TCP/IP network. With the DNS name resolution technique described in "Storing NetBIOS Names on the Domain Nameserver" on page 266, we cannot have a backup domain controller with the same TCP/IP hostname. One DNS domain file entry must have only one IP address associated with it.

NTS's NBNS (Shadow) supports a full datagram distributor function. Microsoft Windows NT server has a WINS server function and it is similar to NTS's NBNS but WINS doesn't have a datagram distributor function, so we don't recommend WINS as our NBNS.

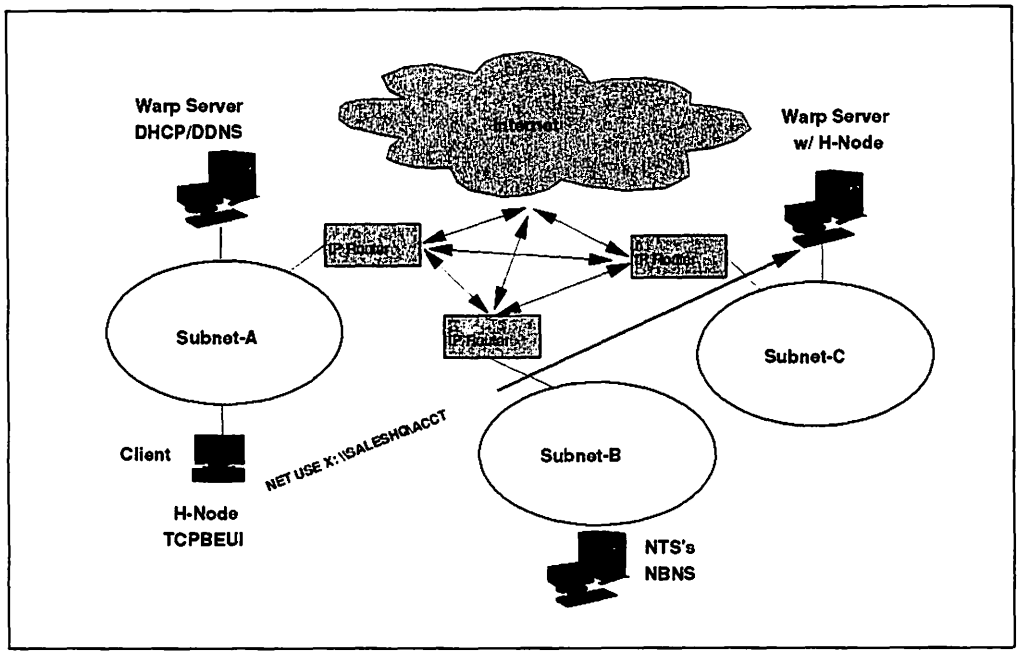


Figure 196. Ideal Solution with DHCP/DDNS plus NBNS

Figure 196 shows the ideal solution for TCP/IP applications such as a Web browser and LAN Server/Clients, over TCP/IP network.

NTS's NBNS (Shadow) has the following requirements:

- Intel 80386 or 80486
- AT compatible EISA or ISA bus
- IDE or Enhanced IDE hard disk
- 8 MB RAM for 16K NetBIOS Names or 16 MB for 64K NetBIOS Names
- FAT 16 File System
- DOS 6.3 or later
- Color Monitor, VGA
- LAN adapter such as IBM's Auto 16/4 Token-Ring ISA Adapter P/N 92G7632

Shadow runs on DOS but it runs just like a network operating system and it effectively uses the LAN adapter card interface and hard disk interface as fast as possible.

There can be a remote control station for Shadow running on top of Windows with NTS's TCPPro program, or IBM OS/2 TCPBEUI workstation's WIN-OS/2 program. The following screen capture shows an example of an NBNS remote manager.

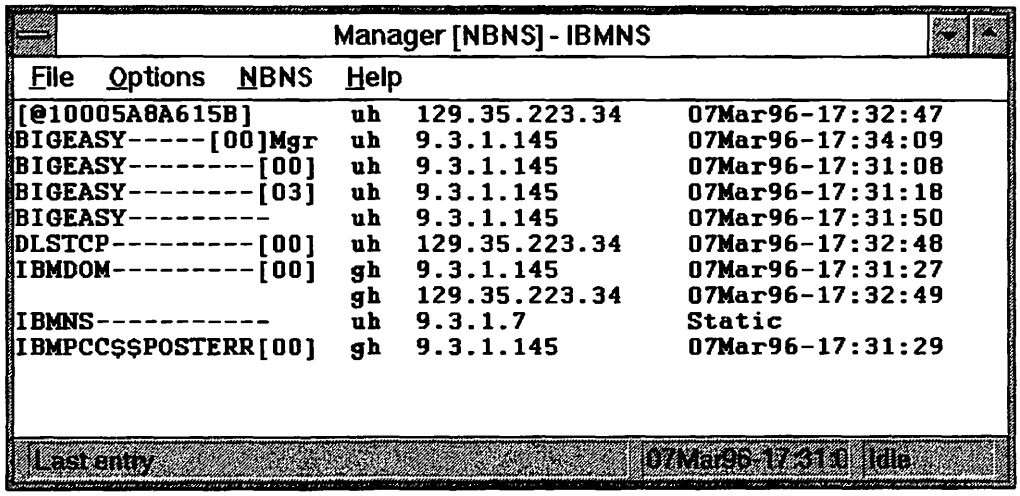


Figure 197. Example of Remote System Manager for NTS NBNS

In Figure 197, domain name IBMDOM has two members, one is 9.3.1.145 which is a LAN Server, the other is 129.35.223.34 which is a DLS client.

Chapter 7. Remote Access Services

This chapter describes the Remote Access Service in OS/2 Warp Server. Remote Access Services is provided in OS/2 Warp Server by the LAN Distance Connection Server product.

In this chapter we will describe how this component may be used and describe some of the functions using a simple scenario.

It is assumed that you have an understanding of basic LAN terminology. For detailed information refer to the online documentation that comes with OS/2 Warp Server or the documentation referenced at the end of this chapter.

Functional Enhancements

For those users who are already familiar with the LAN Distance Connection Server product the following functions have been added to the Remote Access Services component within OS/2 Warp Server:

- Shared security database, see "Shared User Database" on page 353
- Security user-exit, see "Security User Exit Package" on page 352
- Security Database tools, see "Security Database Tools" on page 354
- Inactivity Timeout, see 7.9, "Inactivity Timeout Feature" on page 323
- Updated Modem and Adapter List, which is included in the online documentation

A service pack will be available to include the above enhancements to existing LAN Distance Connection servers. There have been no major enhancements to the LAN Distance clients.

7.1 Overview and Concepts

The Remote Access Services allows multiple, concurrent, remote OS/2 and Microsoft Windows workstations to connect into a LAN. When connected, the remote workstation has the same abilities and functions as if it was directly connected to the LAN and can directly access any device on the LAN.

© Copyright IBM Corp. 1996

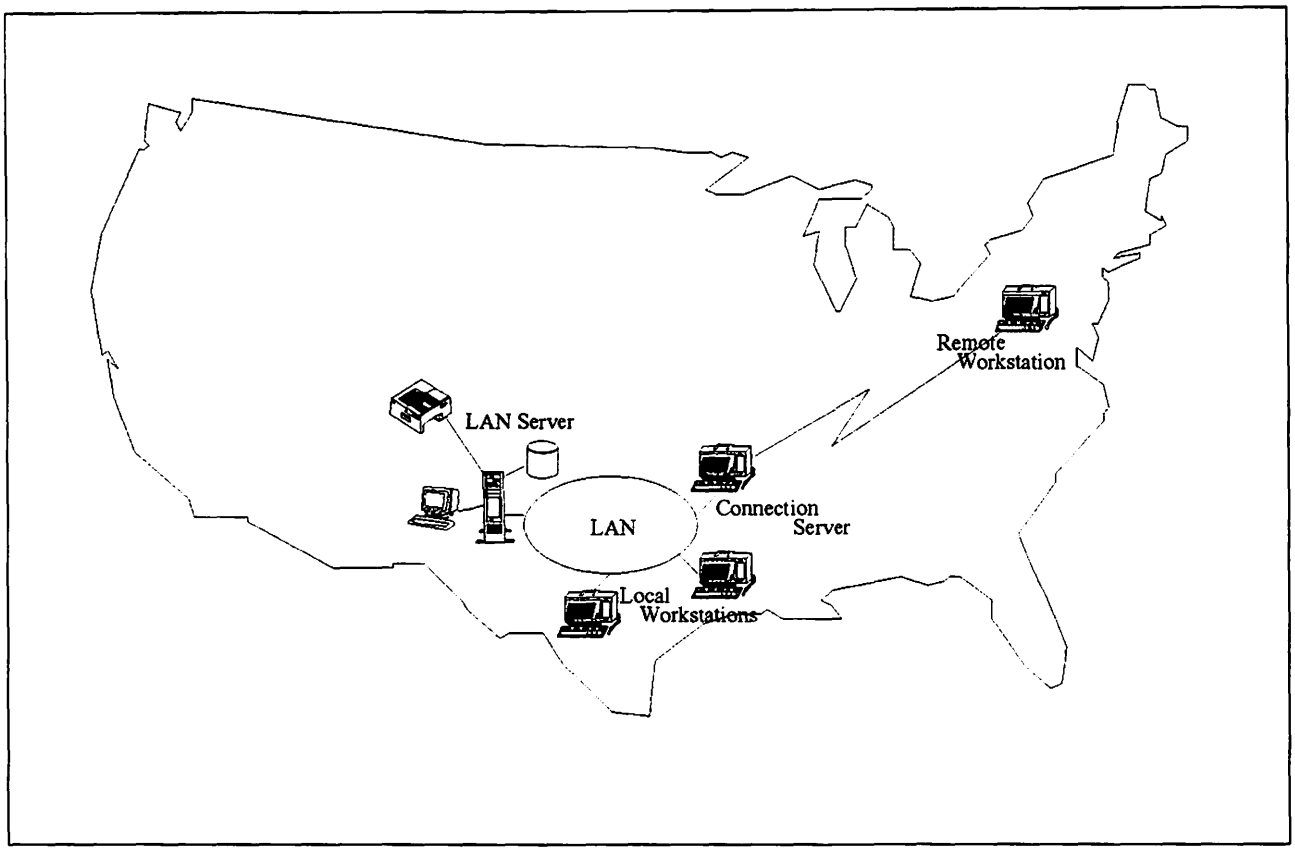


Figure 198. Remote Access Services Overview

A simplified view of a remote workstation attaching to a LAN is shown in Figure 198. The *remote workstation* as its name suggests is a workstation that is not local to the LAN. The Remote Access Services or *Connection Server* is the component of OS/2 Warp Server that provides the remote workstation access to the LAN. When the remote workstation links into the LAN, it forms a *wide area network (WAN)*. The link between the remote workstation and the Connection Server is known as the *WAN link*.

In this case, all that the remote workstation requires is a COM port and modem. The Remote Access Services must be connected to both the LAN via a LAN adapter and the remote workstation via the communications link.

Remote workstations can access the Remote Access Services via a number of communications methods, including asynchronous and synchronous over switched and non-switched telephone lines, and ISDN Basic-Rate switched connections. Remote workstations can connect to token-ring LANs and Ethernet LANs. The Remote Access Services also supports access to X.25 networks through asynchronous modems with X.25 Packet Assembler Disassembler (PAD) capabilities.

Notes:

a. An OS/2 remote workstation can have up to two concurrent connections.

b. If the remote workstation is a DOS/Windows workstation, then only one asynchronous connection, using either a switched or non-switched line, can be used. The DOS/Windows workstation cannot use synchronous or ISDN links.

c. Native X.25 support will be provided by third parties, such as WAN Services for OS/2, announced by Eicon Technology.

Remote Access Services Environments

The Remote Access Services supports four types of remote LAN access environments as shown in Figure 199 on page 284:

- **Remote-to-LAN or LAN-to-Remote**

  Probably the most common use of the Remote Access Services is to provide this type of access. The remote-to-LAN environment is a flexible solution for users requiring access to resources from remote locations, such as home or while traveling. Users can dial the Remote Access Services on their office LAN and run the same applications remotely that they use in the office.

  Alternatively, LAN-attached workstations can request the Remote Access Services server to establish a connection with a remote OS/2 workstation. This could possibly be used when someone in a central office needs to send an updated file to a number of remote workstations. They could dial out through the Remote Access Services and copy the update to each remote workstation in turn.

- **Remote-to-Remote**

  Two remote clients can establish a WAN connection using Remote Access Services, as shown in the Remote-to-Remote Environment, to form a virtual LAN. The remote-to-remote environment is a simple, low-cost solution for stand-alone workstations that require direct access to resources on other stand-alone workstations. For example, the remote-to-remote environment can be used in a local office environment in lieu of expensive LAN cabling or by traveling employees who need access to their office workstations.

- **LAN-to-LAN**

  You can establish a connection between two Remote Access Services Servers to form a casual bridge between two LANs as shown in LAN-to-LAN Environments. LAN workstations on LAN A can use the Remote Access Services connection to access LAN resources on LAN B as if they were physically attached to LAN A. Similarly, LAN workstations on LAN B can access resources on LAN A.

- **Remote-to-Central Server (No LAN)**

  Remote Access Services can be installed as a stand-alone server to support up to 32 workstations. No LAN hardware is necessary on the server, and the remote workstations can all access all the resources at the server.

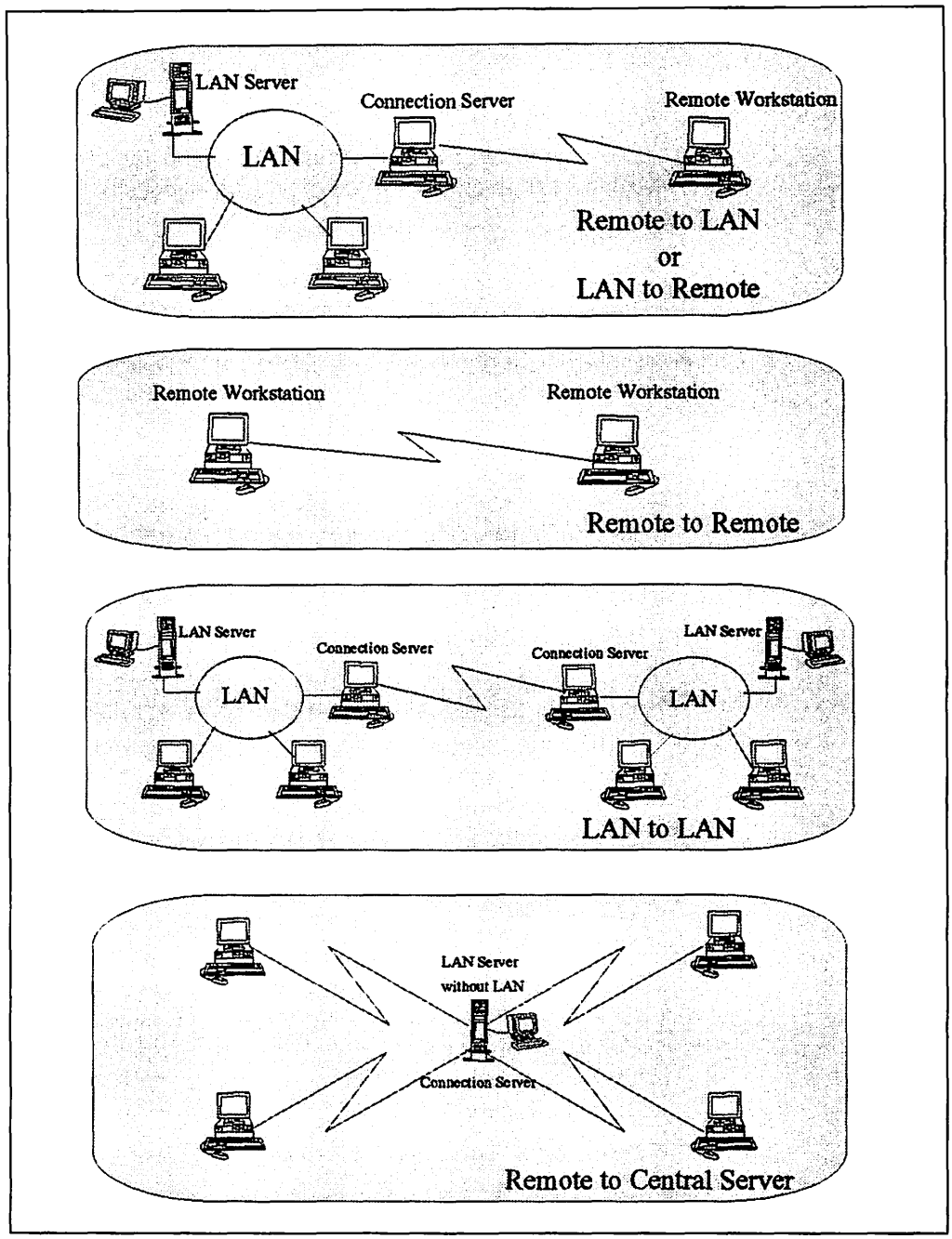


Figure 199. Remote Access Services Configurations

Remote Access Services Clients

The Remote Access Services component within OS/2 Warp Server supports both OS/2 and Microsoft Windows clients. The Remote Access Services client contained within OS/2 Warp Server is equivalent to the LAN Distance Remote client. No major enhancements have been made except for the addition of outstanding fixes. A fixpack will be available for existing LAN Distance Remote clients. In summary the Remote Access Services supports the following clients:

- LAN Distance Remote Clients included in OS/2 Warp Server
- LAN Distance Remote for OS/2 Version 1.x
- LAN Distance Remote for Windows Version 1.x

- OS/2 Warp Connect

7.2 System Requirements

Listed below is the system requirements for the Remote Access Services Server and the Remote Access Services Client. These requirements are for the products alone and does not take into consideration any of the other components of OS/2 Warp Server.

Remote Access Services Server

- IBM OS/2 Version 2.0 (or later).
- Install the network operating system software and any LAN applications that you will run on the Remote Access Services Server.
- Remote Access Services requires 5.0 MB of fixed-disk storage space. Additional disk space is required to install FFST/2 (700 KB) and required LAN transports (2.2 MB), if these products are not already installed.

  The amount of memory recommended for running the Remote Access Services product, OS/2, and one LAN application is 12.0 MB. The requirements for your Remote Access Services Server may vary depending on your LAN applications, data and response time requirements, and your workstation's processor speed.
- Verify that the LAN adapter for the Remote Access Services Server is supported by the Remote Access Services product.
- A modem and/or adapter for asynchronous, synchronous, or ISDN communications. To view a list of supported modems and adapters do the following:

  1. View the A3T11MST.INF file located in the \CID\SERVER\BOOKS directory of the OS/2 Warp Server CD-ROM.
  2. Expand the tree named Hardware Supported for the LAN Distance Remote Product.

  If you are using an adapter for asynchronous or ISDN communications, install and configure the adapter using the adapter software, according to the manufacturer's instructions.
- Access to a switched or nonswitched (leased) telephone line to establish an asynchronous, synchronous, or ISDN connection.
- The following are additional planning considerations for setting up the Remote Access Services Server.
- WAN adapters used by the Remote Access Services Server product cannot be used by other applications simultaneously.
- If Communication Manager/2 is installed on your workstation and you plan to set up an ISDN connection, set up Communications Manager so it is not configured for ISDN.

Remote Access Services Client

The system requirements for the Remote Access Services Client are as follows:

- IBM OS/2 2.0 or later, or Microsoft Windows Version 3.1 running on DOS Version 5.0 or higher.
- 5.0 MB fixed-disk storage. Additional space is required to install First Failure Support Technology/2 (700 KB) and required LAN transports (2.2 MB) if these products are not already installed.

  To run the Remote Access Services client product, OS/2, and one LAN application you need about 12.0 MB memory. The requirements for your workstation may vary depending on your LAN applications, data requirements, processor speed, and response time requirements.
- The MS Windows Remote Access Services product requires 2.3 MB fixed-disk storage.
- A modem and/or adapter for asynchronous, synchronous, or ISDN communications.

  WAN adapters used by the Remote Access Services client product cannot be used by other applications simultaneously.
- Access to a switched or nonswitched (leased) telephone line to establish an asynchronous, synchronous or ISDN connection.
- If you are using an adapter for asynchronous or ISDN communications, install and configure the adapter with the adapter software using the manufacturer's instructions.
- If you have IBM's Communication Manager installed on your workstation and you plan to set up an ISDN connection, set up Communications Manager so it is not configured for ISDN.
- To run your COM ports at a speed greater than 9600 bps, your workstation should have FIFO buffering. However, some non-FIFO workstations with a faster processor (25 MHz and above) and modem (14400 bps or better) can support higher transmission speeds.

  To verify that your workstation has FIFO buffering issue the command `MODE COM1` at an OS/2 command prompt. If the response is `BUFFER = N/A`, then your workstation does not have FIFO buffering. Following is a possible response from the `MODE COM1` command:

```
baud     = 14400          parity   = NONE
databits = 8              stopbits = 1
TO       = OFF            XON      = OFF
IDSR     = OFF            ODSR     = OFF
OCTS     = OFF            DTR      = ON
RTS      = ON             BUFFER   = AUTO
```

7.3 Setting Up the Remote Access Services

Due to the versatility of the Remote Access Services component many different configurations are possible. We will describe setting up the most common scenario as depicted in Figure 200 on page 287.

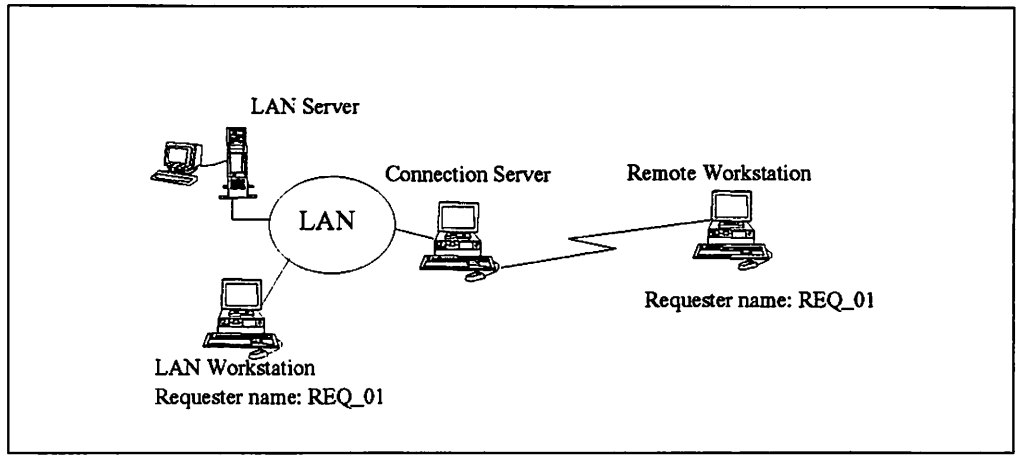


Figure 200. Simple Remote Access Services Configuration

We will perform the tasks in the following order:

1. Install the *Remote Access Services* within OS/2 Warp Server The Remote Access Services server is also know as the Connection Server. We will use these terms interchangeably.
2. Configure the Connection Server.
3. Install and configure the LAN Workstation (REQ_01) to be used as a Remote Workstation.

Installing the Remote Access Services

If you chose to install the Remote Access Services from the main OS/2 Warp Server installation screen you will be presented with the following panel as shown in Figure 201 on page 288

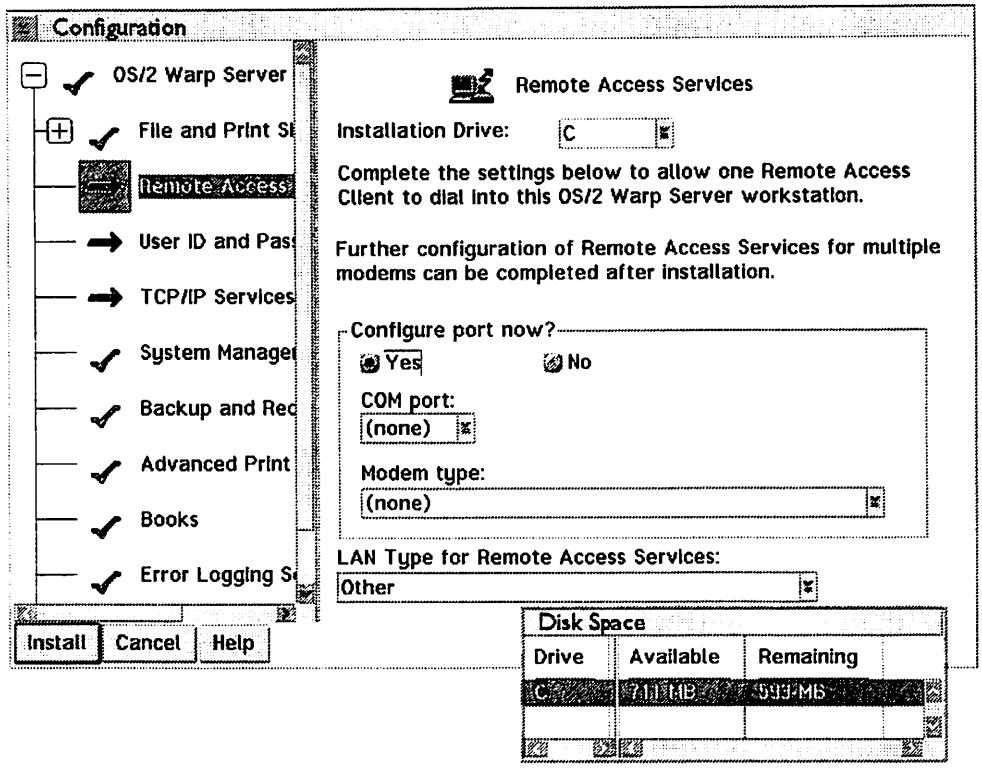


Figure 201. Remote Access Services Configuration/Installation Panel

You will need to specify the drive where you will install the product. You may choose to configure the COM Port now or later. It is best not to configure the COM Port now if:

- Your modem is not listed in the Modem type list
- You wish to make use of a port other than the standard communications ports on the server

If you choose to install the Remote Access Services component later or on another machine you may use the diskette images provided. You may do this either by using a redirected drive or by manually creating the diskettes. The installation program works properly for either procedure. To install the product, follow these steps:

1. Ensure that the media/drive you are installing from is available.
2. At an OS/2 command prompt, run the installation program by issuing the following command:

   `x:\INSTALL`

   Where x is the drive letter you are installing from.

   Note: If you want to install from the OS/2 Warp Server CD-ROM, issue the `INSTALL` command from the \CID\SERVER\LDCS\LO319A1 directory.
3. At the Installation window select **OK**.
4. At the Welcome window select **OK**. The Target Drive window will be presented.
5. Select **Quick Start** for a list of minimal steps necessary to complete installation.

6. At the Target Drive window enter the drive you want Remote Access Services to be installed. Select **OK**. The code is being copied to the target's drive \WAL directory.
7. Follow the instructions, and insert the appropriate Remote Access Services installation diskettes when prompted to do so.

   After the Remote Access Services software has been installed, you will be informed that FFST/2 was installed or updated on this workstation.
8. Select **OK**.

   At this point your CONFIG.SYS and PROTOCOL.INI files have been updated. You will now get a notification screen informing you that the installation has been successfully completed and a shutdown is required.
9. Select **OK** to exit the Remote Access Services installation.
10. Shut down and reboot your system.

The installation program makes the following changes to your system:

- The \WAL directory is created and the Remote Access Services files together with the user configuration files are stored here.
- Changes are made to the CONFIG.SYS and PROTOCOL.INI files.
- After rebooting the workstation you have a *LAN Distance Remote Access* folder on your OS/2 Desktop.
- Installation information is saved in the OS2\INSTALL directory. The WALINST.LOG file contains Remote Access Services installation messages and the LAPSHIST.LOG contains MPTS installation messages.

Table 65 lists the changes that are made to the CONFIG.SYS and PROTOCOL.INI files.

Table 65 (Page 1 of 2). Remote Access Services File Changes

FILE	BACKUP	CHANGES
CONFIG.SYS	d:\CONFIG.WAL	• The WAL directory is added to your path specifications for: – LIBPATH – DPATH – PATH • The Remote Access Services help screens are added to the HELP specification. • The specifications for the Remote Access Services device drivers are added. • The device drivers for LAPS and NetBIOS are added. • If FFST/2 is installed during Remote Access Services installation, appropriate statements for it are added. • Statements for the locked file device driver are added temporarily to the top of your CONFIG.SYS file. The statements are removed the next time you start your workstation.

Table 65 (Page 2 of 2). Remote Access Services File Changes		
FILE	**BACKUP**	**CHANGES**
d:\IBMCOM\PROTOCOL.INI	d:\WAL\PROTOCOL.WAL	• If NetBIOS is installed during Remote Access Services installation, a section for NETBEUI_NIF is added. • Your NetBIOS timers are adjusted. • The number of NetBIOS NCBs, names, and sessions are increased (if not already done so by the OS/2 Warp Server Tuning Assistant). • A section is added for VLAN_kernel. • A section for PDFH_NIF is added.

7.4 Configuring Remote Access Services

Once you have successfully installed Remote Access Services a LAN Distance Remote Access folder will appear on your desktop. Within this folder you will have an IBM Remote Access icon. If you select this icon you will be presented with the *LAN Distance - Workstations* as shown in Figure 202.

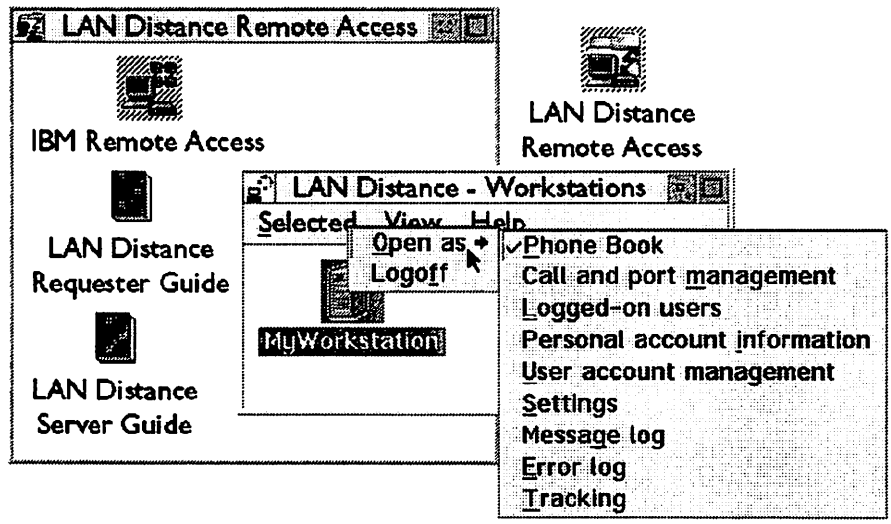


Figure 202. Remote Access Services Configuration Action Items

Notice that there is on icon in this window that looks like a server and is labeled `MyWorkstation`. This icon represents the workstation where you have just installed Remote Access Services. If there are other Remote Access Services or remote workstations on the same LAN, you will also see icons representing these machines. By selecting this icon and clicking on the right mouse button, or from the menu bar select Selected and open as, you will be presented with a menu which contains a number of action items. These action items are used to configure, view and track the Remote Access Services server.

Once security has been enable on a the Remote Access Services server only the actions you are authorized to perform are listed in the pull-down menu.
Table 66 on page 291 shows what the purpose of each action item is and who is authorized to use it.

Remote Access Services Actions describes all the action windows that can be included in the Open as → menu. The user type required for each action window is also listed. This becomes effective once security has been enabled.

Note: Personal account information and User account management information will only be presented if you are successfully logged on to the Remote Access Services server.

Table 66 (Page 1 of 2). Remote Access Services Action List

Open as →	Action
Phone Book	Establish connections to LANs and other workstations. The phone book is your dialing directory. It contains phone book entries for the information needed to establish connections. Double clicking with mouse button 1 on MyWorkstation also opens your Phone Book window. Required privilege: user
Call and port management	View and manage the calls established through the work station. Also, stop and start your port managers. Required privilege: user
Logged-on users	View the users that are logged on to the workstation. This action window is available only on secure workstations. Required privilege: user
Personal account information	Manage your personal account on the workstation. View your passphrase status and, optionally, change your passphrase and your personal account description. This action window is available only on secure workstations. Required privilege: user
User account management	Manage the workstation security policy and its user account database. Set up a user account database to designate which users are allowed to remotely access the workstation or LAN. This action window is available only on secure workstations. Required privilege: Security Administrator
Settings	The Settings notebook contains many pages. Five of its tabs lead to other notebooks: • Phone Book • Answer • Ports • Modems • Bridge Configuration changes you make in the Settings notebook or its imbedded notebooks are not saved until you close the Settings notebook. You can view and work with all of your changes while the notebook is open. When you close the Settings notebook, choose whether to accept or delete your changes. The Settings notebook can be opened by any user. On a secure workstations, the Settings notebook displays only the tabs that are granted to the user who opens the notebook. For example, the notebook includes only the Information tab for a *user*. If an administrator opens the notebook, all of the tabs, except Security are available.

Table 66 (Page 2 of 2). Remote Access Services Action List	
Open as →	**Action**
Message log	View error and warning messages generated by the Remote Access Services product. Use the message log to investigate and correct Remote Access Services configuration and connection problems. Contact your designated support organization for additional help if you cannot resolve a problem with the product. Required privilege: user
Error log	Access the OS/2 error log facility and view the errors logged there by the Remote Access Services product. The information in the OS/2 error log is in hexadecimal format. It is intended to help your designated support organization resolve error situations. Required privilege: user
Tracking	Access information and tools for problem determination, including the audit log. Tools include trace, dump, and file retrieval facilities. On a secure workstation, the Tracking notebook displays only the tabs that are granted to the user who opens the notebook. For example, a *user* cannot access an audit log, so the Audit tab is not displayed for a *user*.

Before the Remote Access Services can be used, it must first be configured. The following steps must be completed to configure a basic Remote Access Services Server to provide access to a single remote workstation. The steps are presented in more detail in the following sections:

1. Open the Remote Access Services **Settings** notebook.
2. Configure the WAN **Ports**.
3. Configure the **Modems**.
4. Configure the **Bridge**.
5. Configure the **Address/LAN**.
6. Configure the **Answer** modes.
7. Configure the **Workstation**.
8. Configure the **Phone Book**.
9. Reconfigure **LAPS** (MPTS).
10. Save the configuration and restart the workstation.

Open the Remote Access Services Settings Notebook

The Remote Access Services is configured through a Settings Notebook. To get to the Settings Notebook you first need to start Remote Access Services.

Figure 202 on page 290 shows you the LAN Distance-Workstations window. To open the Settings notebook for your Remote Access Services, follow these instructions:

1. Select the icon representing your Remote Access Services, with the right mouse button (see Figure 202 on page 290).
2. Select **Selected** from the menu bar.
3. Select **Open as →**.
4. Select **Settings**.

   The LAN Distance Settings notebook is displayed as shown in Figure 203. This notebook is used to configure Remote Access Services

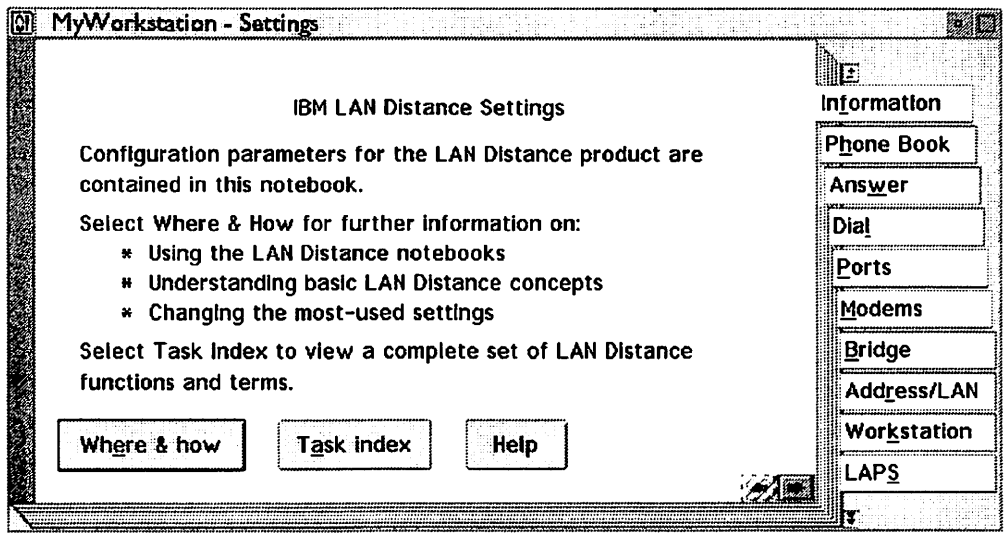


Figure 203. LAN Distance Settings Window

Configure the WAN Port

The WAN port is the path that the Remote Access Services will use to communicate with the remote workstations. It is the access point for connections to and from your server. Calls are dialed and answered through these ports. Generally speaking, one port is required for every modem, internal or external, on your server.

You need to configure one port for every modem on the connection server. You can define a port as being of one of the following types:

- Asynchronous and synchronous ports for ARTIC adapters with external modems
- Asynchronous COM ports with internal or external modems
- ISDN ports (set up using the ISDN support program)
- ISDN Waverunner modem

A number of ports can be configured depending on your hardware configuration, your WAN environment, and your requirements. In this case, we configure only one WAN port to use with an asynchronous modem.

Follow these steps to configure the WAN port:

1. From the LAN Distance Settings notebook, select the **Ports** tab.
2. From the notebook page, select the **Add...** button. This will display the window as shown in Figure 204 on page 294

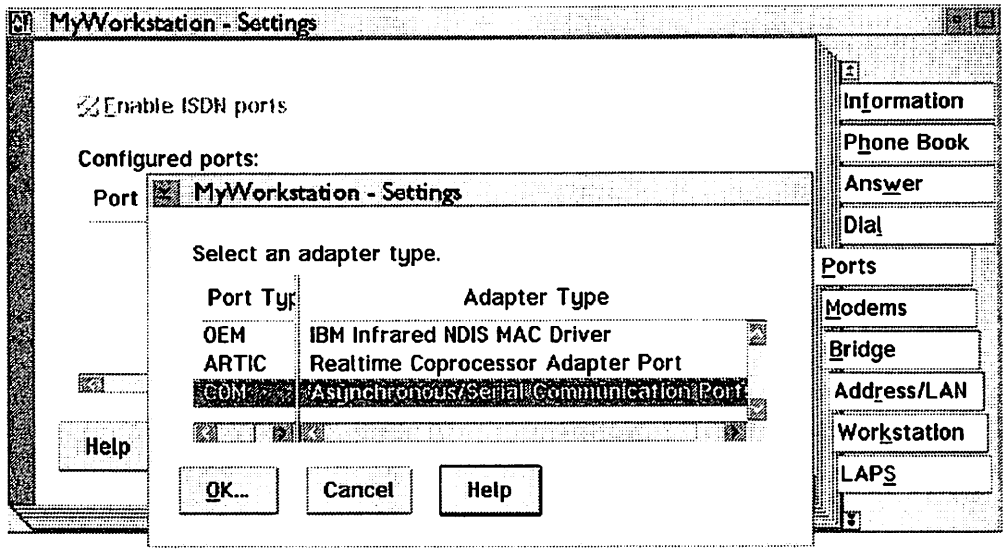


Figure 204. Settings Window - Add Port

3. Select the port type you are using.

   In this case we are using an asynchronous modem via a COM port.

4. Select the **Asynchronous/Serial Communication** line from the list box as shown in Figure 204..

5. Select the **OK** button.

   The COM Port - Settings window is displayed, as follows:

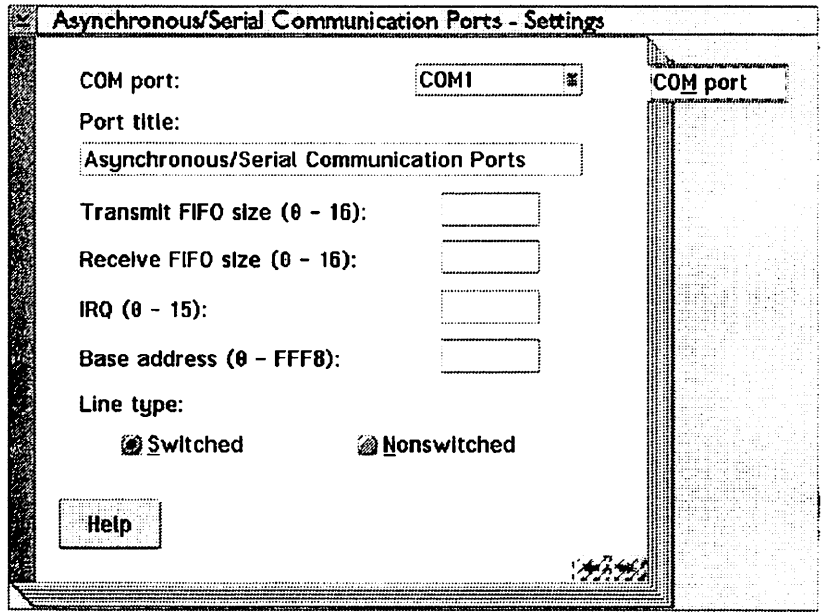


Figure 205. COM Port - Settings Window

6. All the defaults can be accepted.

   The fields presented in the COM Port - Settings window do not generally need to be changed. In most cases, Remote Access Services queries the COM port hardware in your workstation and uses it effectively. If you enter

values into any of these fields, you must be certain they are accurate. Otherwise Remote Access Services may not function correctly.

Because we are using an asynchronous modem, we can accept the default line type of **Switched**. If the Remote Workstation and Remote Access Services are connected via a leased line, or directly connected via their asynchronous COM ports, then **Nonswitched** would be selected (for example, if you are using a null modem cable).

7. Close the **COM Port - Settings** window.

   Select the system icon at the top-left corner of the notebook, and then select **Close**.

Configure the Modem

If you are using a modem to connect into the WAN, then it must be configured and attached to a WAN port. Follow these steps to configure a modem:

1. Select the **Modems** tab from the Settings notebook. Then select the **Assign...** button. A list of modems is displayed.

   The following window is displayed:

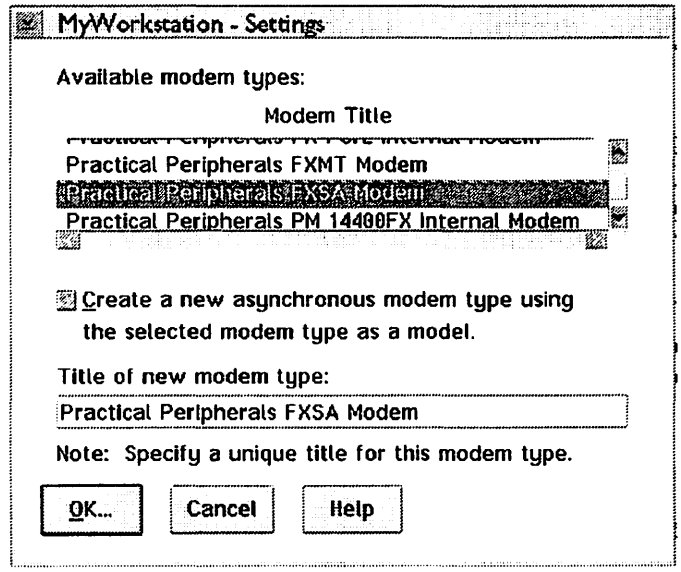

MyWorkstation - Settings
Available modem types:
Modem Title
Practical Peripherals FXMT Modem
Practical Peripherals FXSA Modem
Practical Peripherals PM 14400FX Internal Modem
Create a new asynchronous modem type using the selected modem type as a model.
Title of new modem type:
Practical Peripherals FXSA Modem
Note: Specify a unique title for this modem type.
OK...
Cancel
Help

Figure 206. Settings Window - Select Modems

2. Select a modem from the Available modem types list box.

   In our environment, we are using a Practical Peripherals FXSA Modem.

   Note: If your modem is not listed in the Available modem types list box, you must configure a new modem type. It is critical to the operation of Remote Access Services that all modems used by Remote Access Services in the WAN are set up correctly.

   An unlisted modem can be configured with the CFMODEM utility (shipped with OS/2 Warp Server) by:

   - Creating a new asynchronous modem type using an existing modem as a model.

     Using this method, you must select a modem that is similar in operation and function to your modem. The existing modem definition is copied,

creating a new entry in the list. Now you modify the modem setup with the help of your modem user's guide.

- Creating a PIF file for your unlisted modem using the PIF file of a listed modem as a template.

  See 7.14, "PIF Files for Uncertified Modems" on page 363 for more information.

3. Select the **OK...** button.

   The following Practical Peripherals FXSA Modem - Settings notebook is displayed.

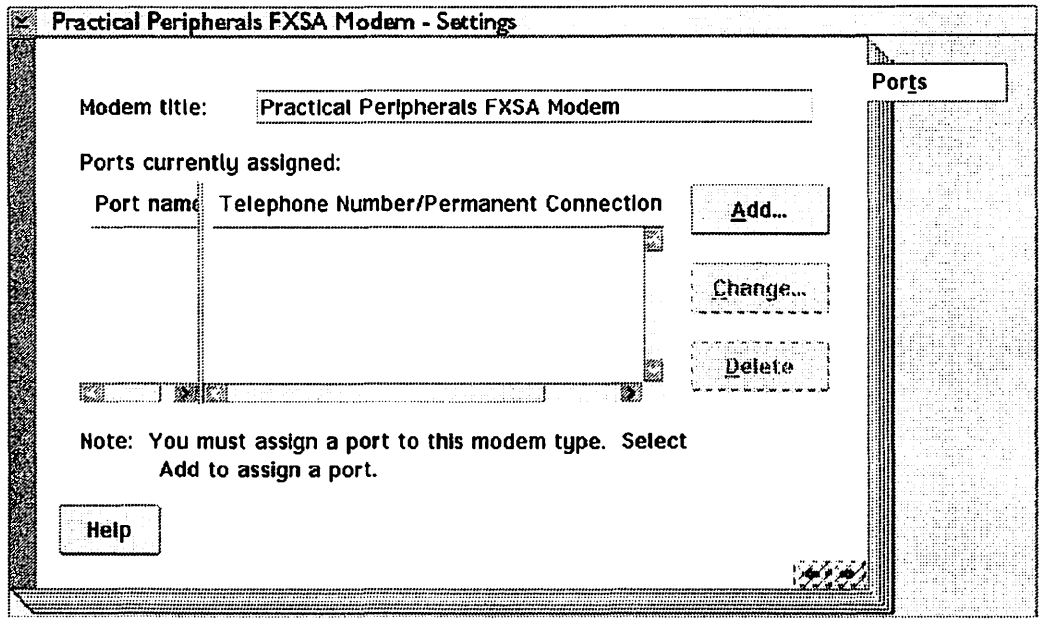


Figure 207. Practical Peripherals FXSA Modem - Settings Window (Add Modem)

4. Select the **Add...** button.

   You are presented with a window that allows you to enter either a phone number or a permanent connection name. These two fields are comment fields that become part of the phone book/answer mode entries and are used to help select a specific port to make a connection on. (If you enter nothing here, then **Unspecified** is generated for those entries.) We recommend that you fill in these fields. Then later, in the call and port management, there will be information that represents your system environment and makes it easier to manage your ports.

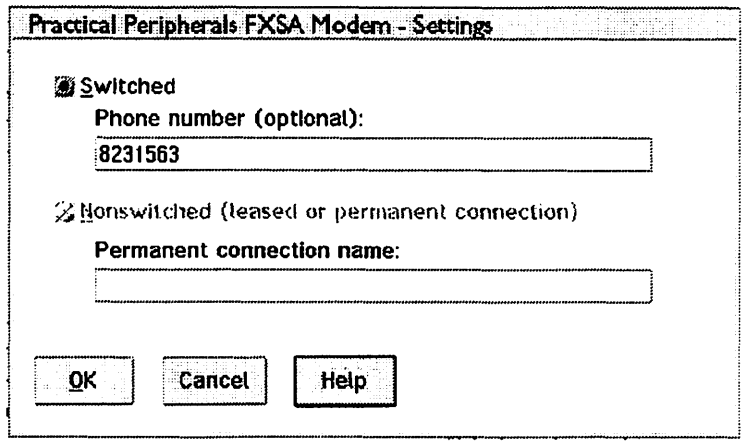


Figure 208. Practical Peripherals FXSA Modem - Settings Window (Phone Number)

5. Enter the phone number to be dialed by a Remote Workstation in order to connect to the Remote Access Services via this modem and port.

   The phone number identifies the specific modem and port that Remote Workstations dial to communicate with this Remote Access Services. This will be displayed later in the call and port management, allowing you to see which line is in use.

6. Select the **OK** button.

   You must now select the port to which this modem is attached. In this window you see ports that previously have been added. If you remove a port later, the modem will be removed too.

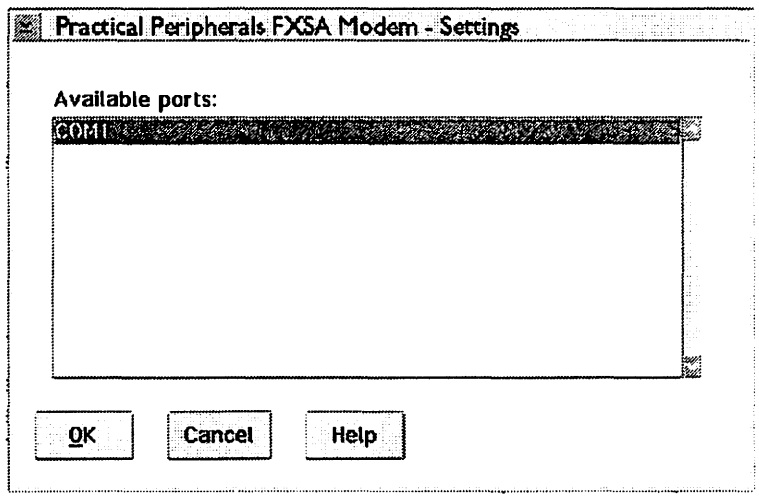


Figure 209. Practical Peripherals FXSA Modem - Settings Window (COM Port)

7. Select **COM1**.
8. Select the **OK** button.

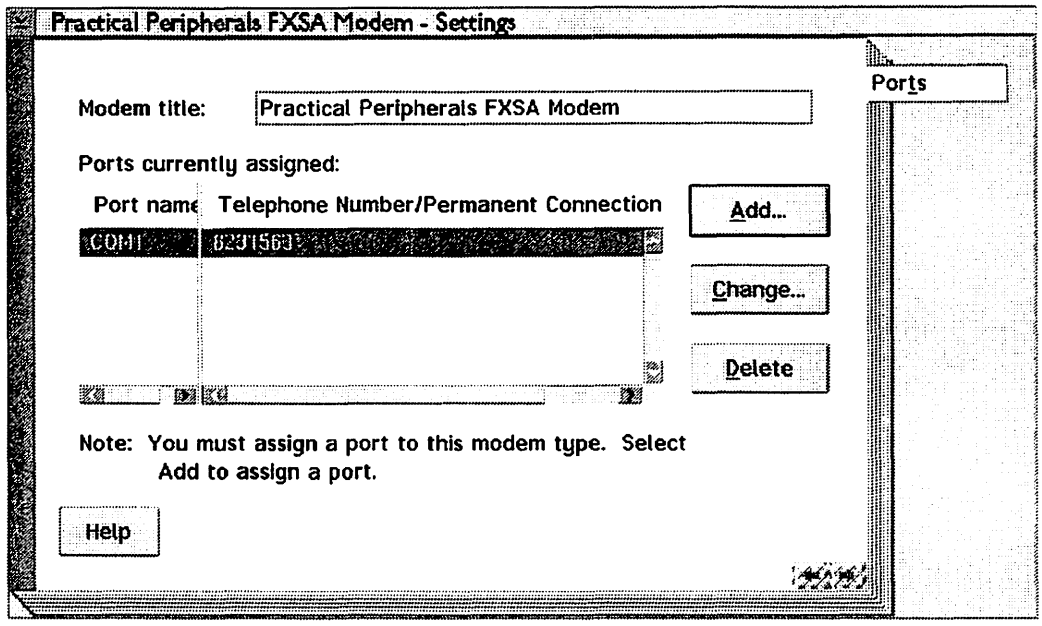


Figure 210. Practical Peripherals FXSA Modem - Settings Window (Assign Modem to a Port)

Figure 210 shows you the modem type and the port it is assigned to. The phone number is the number a Remote Workstation must dial to connect to this Remote Access Services. If the same modem type was connected to COM1, COM2, and COM3, then each port would be shown along with the phone numbers to dial.

9. Close the window to finish the modem configuration.

   Note: The assignment of a port to a modem type provides the association between your logical ports and your physical WAN hardware. One modem type can have multiple ports assigned to it as long as there is physically one modem attached to your system for each port defined.

Configure the Bridge

The Remote Access Services bridge is located on the Connection Server and is used to route LAN frames between Remote Workstations in the WAN and the LAN. In a token-ring network, this bridge functions as a *source routing bridge* such as the IBM Token-Ring Bridge Program. In an Ethernet network, the bridge functions as a *transparent bridge*. This bridge cannot be used as a *translation bridge*, that is, you can only connect the same type of networks together. It is not possible to connect a token-ring LAN with Ethernet LAN using the this bridge

Because this bridge functions as a *normal* bridge, it must be configured in a similar way. Follow the steps below to configure the Remote Access Services bridge:

1. Select the notebook tab **Bridge**.

   The following window is displayed:

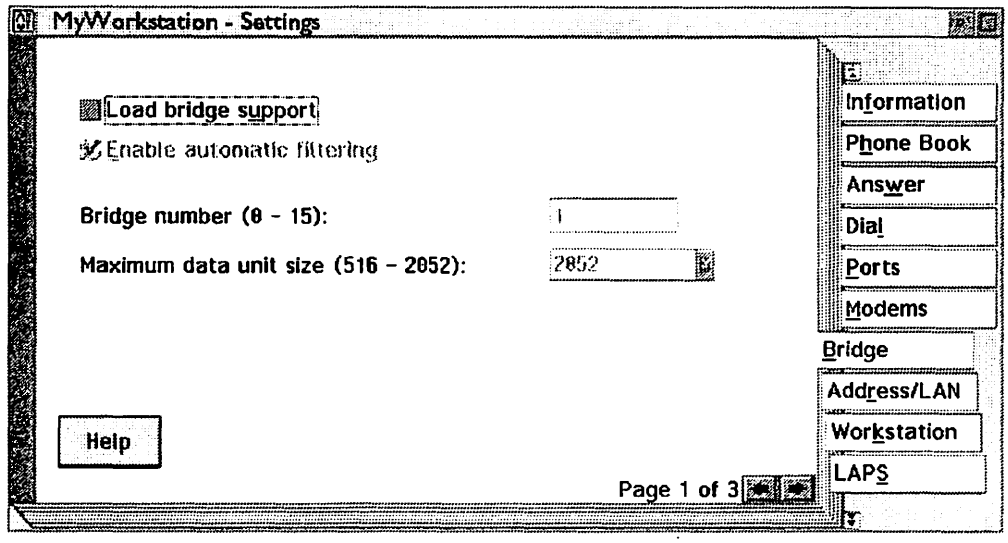


Figure 211. Settings Window (Bridge Section: Page 1 of 3)

2. Accept the defaults.

   In the panel shown in Figure 211, you can enable automatic filtering.

   The **Bridge number** identifies this bridge uniquely between two LAN segments. (Note that the WAN, and all devices connected into the Remote Access Services via the WAN, appear as a LAN segment to the bridge). If there are multiple bridges between the same two segments (that is, parallel bridges), then this bridge number must be unique for each bridge. (Note, parallel bridges are only valid in a token-ring LAN, not Ethernet.)

   Note: The bridge number, LAN segment ring number, and WAN segment ring number combine to form a route designator for LAN data frames. The route designator must be unique on the wide area network. If the Remote Access Services is part of a large and complex LAN environment, then these numbers must be coordinated. One way to ensure that the route designator is unique in a smaller network is to assign different bridge numbers to each of the Remote Access Services bridges in your system.

   The **Maximum data unit size** specifies the largest size for LAN frames that can pass through this bridge. If your connection server bridge receives a data frame that exceeds this maximum size, the frame is discarded. In general, it is recommended that the largest data unit that can be transmitted by the connection server bridge be specified. Consider the following tradeoffs when setting this limit:

   - A large data frame incurs less overhead for the amount of data being transmitted.
   - Transmission errors might not have as big of an impact if you send small data frames.

3. Select the next page arrow to go to Page 2 of 3.

   On page 2, you can set the local LAN segment number, the maximum number of network bridge hops and active filters.

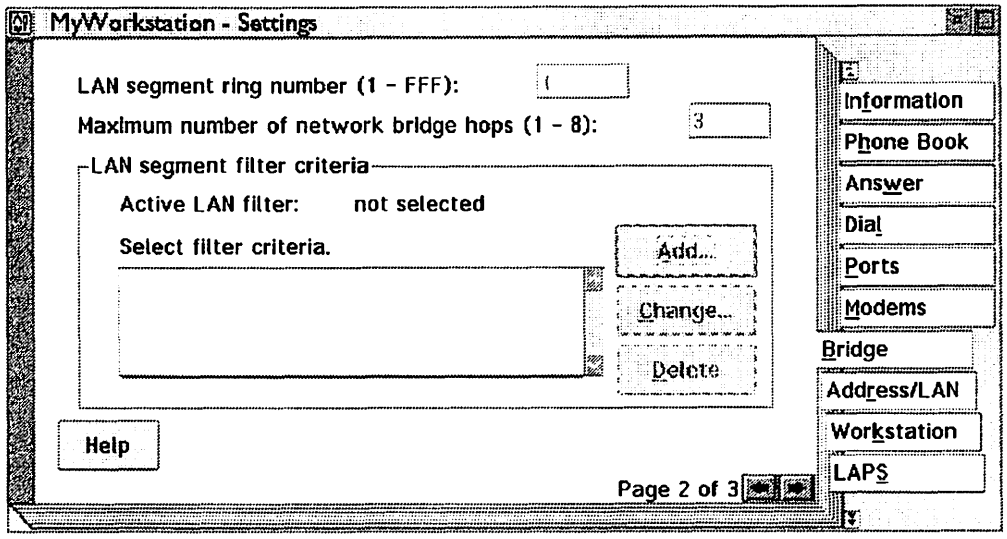


Figure 212. Settings Window (Bridge Section: Page 2 of 3)

4. Enter the **LAN segment ring number**.

   The **LAN segment ring number** is the ring number of the LAN segment on which your Connection Server workstation resides. If your LAN segment is stand-alone or isolated (not bridged) from any other LAN segment, then the value you enter here can be anything within the valid range. If you are adding a number of Remote Access Services' to the local LAN segment, then this number must be the same for each Remote Access Services. If your LAN segment is part of a large network, then you need to obtain this segment number from your network administrator or use OS2PING/CALLBRDG to discover it.

   Note: It is most important that the local LAN segment number, and the WAN segment number be managed correctly. As more Remote Access Services' are added to the LAN/WAN system, or the network grows larger, these segment numbers become more important.

   Filtering Hint

   An easy way to prohibit all communication between the Remote Workstations and LAN segments outside of the first LAN segment (where the Connection Server resides) is to define a unique LAN segment ring number on the Remote Access Services. This filters *all* traffic (not only broadcast traffic) on rings outside the local LAN segment.

   The **Maximum number of network bridge hops** restricts the number of network segments that a data frame can traverse before it reaches its destination. A network segment hop occurs at every bridge on your LAN, including the connection server bridge. If the connection server bridge detects that a frame has exceeded the configured hop count, it discards the frame. Set your hop count high enough to compensate for all of the bridges in both your Remote Access Services wide area network and your existing LAN environment. Set your LAN and WAN segment hop counts to the same value.

   Hop counts can be used to filter LAN traffic by limiting transmission of data to a certain geographic area. For example, setting your hop count to 1, stops broadcast frames that originate from LAN segments *other than the locally attached segment* from being forwarded to Remote Workstations on

the WAN. In this case, broadcast frames that are more than one LAN segment (one hop) away are not forwarded to the Remote Workstations.

LAN segment filter criteria allows you to manually restrict data from flowing between the WAN and LAN. These restrictions apply to *all* ports set up on the Remote Access Services.

We will not add customized filtering at this time, since normally you will use the automatic filtering function. If you decide to also set up this customized filtering, keep in mind that the filter criteria you specify will apply to all ports on the Remote Access Services.

5. Select the next page arrow to continue.

   Here, you can set the WAN segment number, the maximum number of network bridge hops, and active filters.

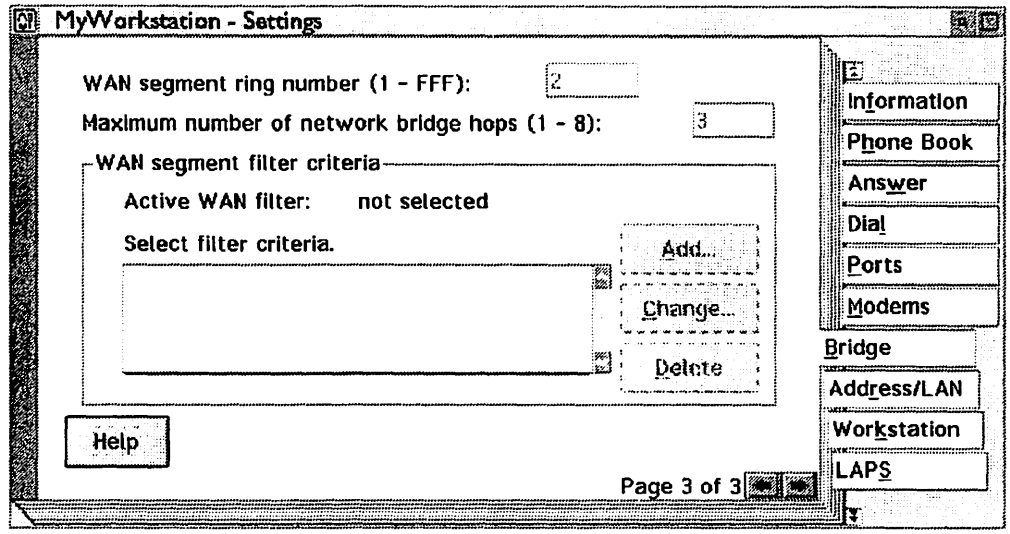


Figure 213. Settings Window (Bridge Section: Page 3 of 3)

6. Enter the **WAN segment ring number**

   The **WAN segment ring number** must be different than your local LAN segment ring number. If the two segment numbers are not unique, the bridge would not be able to route frames from the WAN segment to the LAN segment.

Configure the Network Address

The Remote Access Services server acts as a bridge between two LAN segments. In order for the bridge to operate, it must route frames between the two adapters connected to each LAN segment. The *WAN segment* and *LAN adapter* connected to it, are logical devices. Although the adapter is a logical device, it must still have an adapter address.

The following steps show how to set up the Remote Access Services logical adapter:

1. Select the notebook tab **Address** from the Settings notebook.

   The following window is displayed:

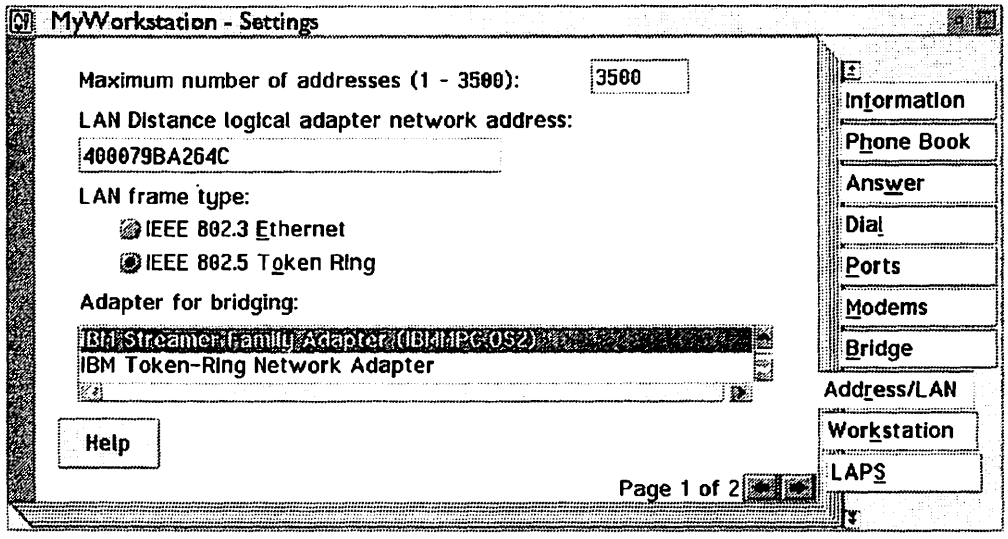


Figure 214. Settings Window (Address Section: Page 1 of 2)

2. Enter the **LAN Distance logical adapter network address**.

   This address should be unique within the LAN/WAN network. If you are setting up a large LAN/WAN environment, then these addresses should be managed centrally and should be based on a standard convention.

   The workstation is assigned a logical adapter network address so that it can be uniquely identified on a Remote Access Services wide area network. During installation of Remote Access Services, you can either specify a logical adapter network address or allow one to be automatically generated. It is not guaranteed that the logical adapter network addresses generated by Remote Access Services are unique. After installation, verify that your logical adapter network address is unique across all segments of your Remote Access Services wide area network. To do this, you can use the OS2PING utility.

3. Leave the other values at their defaults.

   The **Maximum number of addresses** specifies the largest number of workstations and resources that are expected to participate in the Remote Access Services wide area network at any one time. Remote Access Services allocates memory based on this value. If the number of workstations in the WAN exceeds this value, new workstations cannot be added.

   The following workstations and resources are included and should be counted as devices for this value:

   - Remote Access Services workstation
   - Remote Workstations and resources that connect to the Remote Access Services
   - Workstations on the local LAN that communicate with Remote Workstations via the Remote Access Services
   - Resources on the local LAN that are used by Remote Workstations
   - Remote workstations and resources that communicate with other Remote Workstations via Remote Access Services

Note: On page 2 of 2 you are asked about the optional Remote Access Services logical network adapter address. This optional Remote Access Services logical network adapter address is only required if more than five NDIS protocols are used on your workstation.

Configure the Answer Modes

Before the Remote Access Services can be used to receive incoming calls from Remote Workstations, it has to be set up to answer calls. An *answer mode* is an answering state of a workstation based on a set of criteria that determine which incoming calls are accepted. For example, a connection server can be configured to accept calls only over a specific leased line. To accomplish this, the answer mode that includes the name of the leased line in its answer criteria, must be set up. The answer mode on the Connection Server that is to receive incoming calls only on that leased line must then be activated.

Follow these steps to set up the answer mode for the Remote Access Services:

1. Select the **Answer** tab.

   This displays the answer configuration page of the Settings notebook:

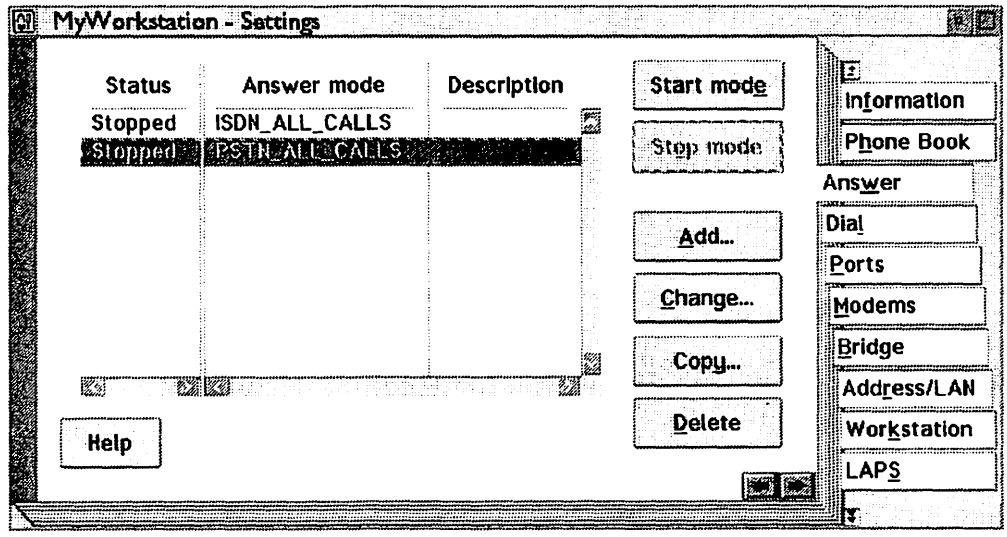


Figure 215. Settings Window (Answer Section: Change Settings)

2. Select the **Stopped PSTN_ALL_CALLS** line.

   Two answer modes are installed, but not initially activated, on your workstation. Both enable your workstation to accept all incoming calls for a particular connectivity. The pre-configured answer modes are:

   - **PSTN_ALL_CALLS** - Public Switched Telephone Network
   - **ISDN_ALL_CALLS** - ISDN

3. Select the **Change...** button.

   This presents another notebook that allows you to set up the answer criteria for the PSTN_ALL_CALLS answer mode.

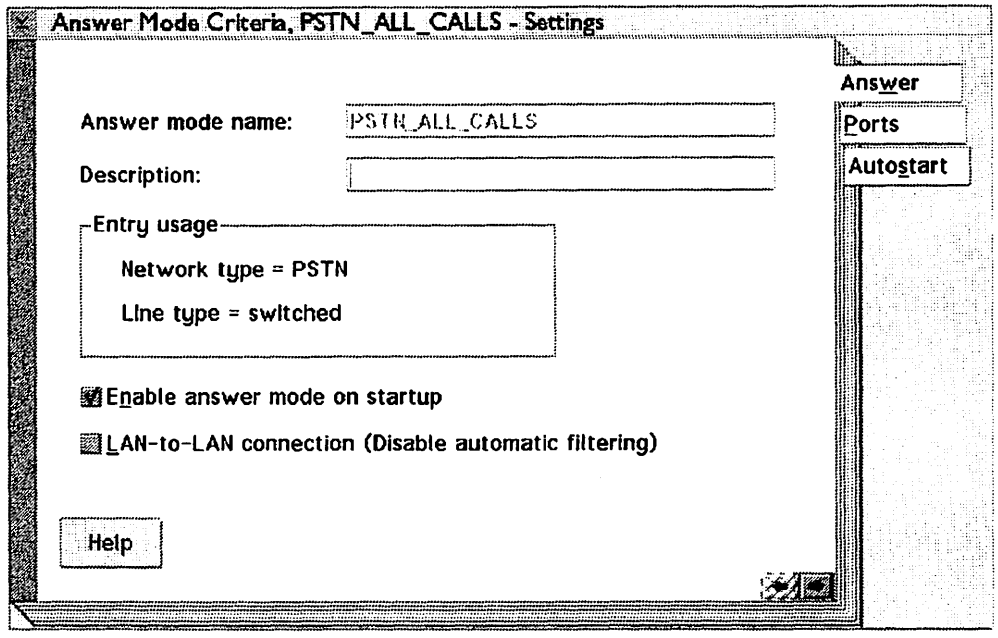


Figure 216. Answer Criteria - Settings Window (Enable Answer)

4. Select **Enable answer mode on startup** (be sure there is a check in the box to the left of that option).

   This sets up Remote Access Services to automatically activate this answer mode every time Remote Access Services is started.

   If you plan to have a LAN-to-LAN connection, you will receive a message telling you that automatic filtering will be disabled. When you check this box it is critical that you set up manual, customized filtering.

   Note: The notebook tabs Ports and Autostart are optional. The Ports tab is available if your workstation is configured to use a modem (PSTN) and a typical telephone line (switched). You can select the **Ports** tab to specify whether to enable all ports or specific ports to answer calls. You can select the **Autostart** tab if you would like to automatically start a program when the connection is established.

   Close the **Answer Criteria** notebook by selecting the system icon at the top-left corner of the notebook, and then select **Close**.

   You are returned to the LAN Distance Settings Notebook.

Configure the Workstation

This enables the name and description of the Remote Access Services to be defined. Initially, after Remote Access Services has been installed, the name MyWorkstation appears under the Connection Server. This name should be changed to something more meaningful to quickly identify the server in the LAN Distance - Workstations window. To change the workstation configuration, follow these steps:

1. Select the **Workstation** tab from the **Settings** notebook.
2. Enter the local Remote Access Services name.
3. Enter the local Remote Access Services description.

   All other options can be left as the default. The window looks similar to the following:

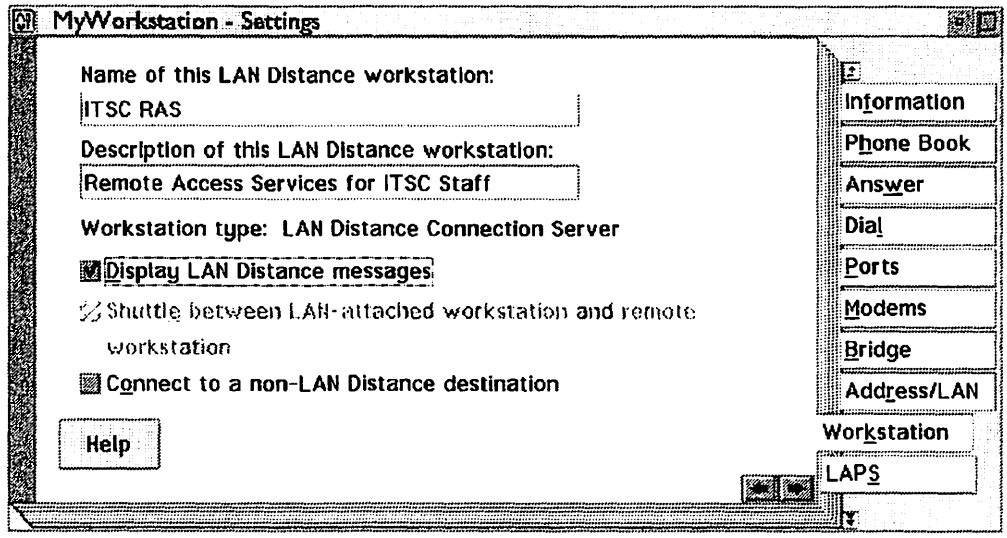


Figure 217. Settings Window (Workstation Section)

Note: **Display LAN Distance messages**. Select this check box to display a notification whenever a Remote Access Services message is generated. If you select this check box, a message notification pop-up window is displayed for each error message posted in your Remote Access Services system.

If you do not require messages to be displayed, deselect the **Display LAN Distance messages** check box.

For example, an unattended Connection Server workstation used only for allowing Remote workstation connections is a good candidate for a system that does not need to display messages. However when a message requires a user response, an unattended Connection Server workstation could interrupt the function of a Remote workstation. Because message notification can delay system processing, use this check box to suppress message notification.

The **Shuttling between LAN-attached workstation and remote workstation** check box is not available for a Connection Server.

Connect to a non-LAN Distance destination. Select this check box to access non-LAN Distance workstations. Use this feature if you are not using security in your Remote Access Services environment. You can set all Remote workstations and Connection Servers to connect to a non-LAN Distance destination, and the system performance will be increased.

Note: All Remote Workstations and Connection Servers must match on this option. That is, *either all are set up to connect to a non-LAN Distance. destination (this box is checked)* or all are not set up to connect *to a non-LAN Distance destination (this box is not checked).*

Configure the PhoneBook

In this section a user is defined in the PhoneBook section as we need the user entry later to set up the security Callback feature. The phone book is normally used on a Remote Workstation to provide a list of Connection Servers that a Remote Workstation can contact. The phone book is also used on the Connection Server to allow call back users, or to call other Remote Workstations.

Follow these steps to configure a user for callback:

1. From the Settings notebook select the **PhoneBook** tab, and then the **Add...** button. Figure 218 is displayed.

   In this window, you have to specify the type of telephone lines and modems you use to call other workstations.

   This window is available the first time you configure a PhoneBook entry. If your workstation is configured for both network and line types, then the window displays every time you configure a PhoneBook entry.

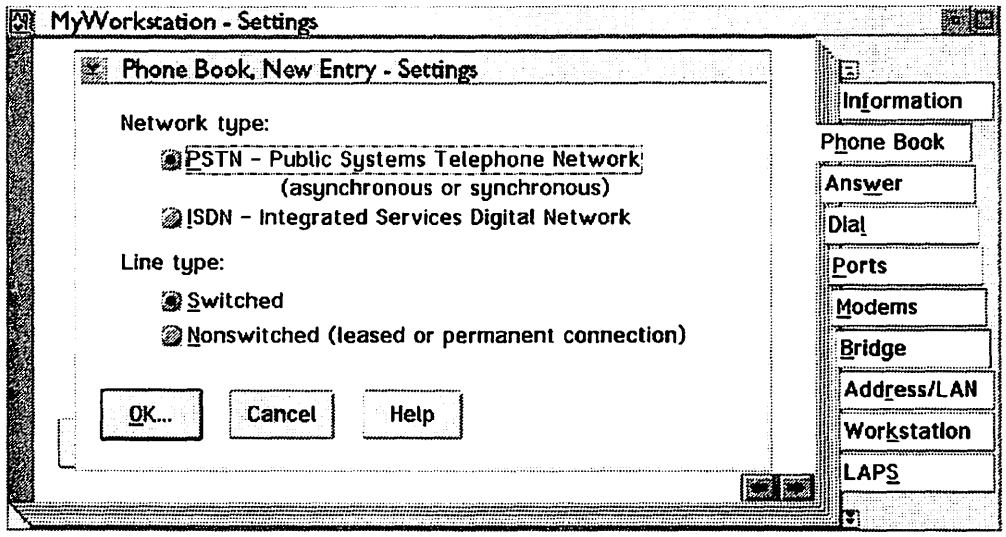


Figure 218. PhoneBook, New Entry - Settings Window

   Note: The PhoneBook entry / Description lists the entries in your phone book, along with their descriptions.

   Phone book entries provide all the configuration information your workstation and its hardware require to call another Remote workstation or to establish a connection with a Connection Server.

2. In the Network type section, select **PSTN**.

   PSTN is used to configure a PhoneBook entry for a workstation you call with a synchronous or asynchronous modem over typical telephone lines. If your workstation only has a modem (and no ISDN adapter), PSTN is automatically selected for you.

   Note: ISDN is used to configure a PhoneBook entry for a workstation you call on an ISDN network. ISDN stands for Integrated Services Digital Network and supports end to end digital voice and data services.

   If your workstation only has an ISDN adapter (and no modem), ISDN is automatically selected for you.

3. In the Line type section select **Switched**.

   Switched is used if you want to call the PhoneBook entry workstation over a regular telephone line. If you selected PSTN on the Network type field, **Switched** is defaulted for you.

   Note: Non-switched is used if you want to call the PhoneBook entry workstation over a leased line or through a permanent connection.

4. Select the **OK...** button.

The following window is displayed:

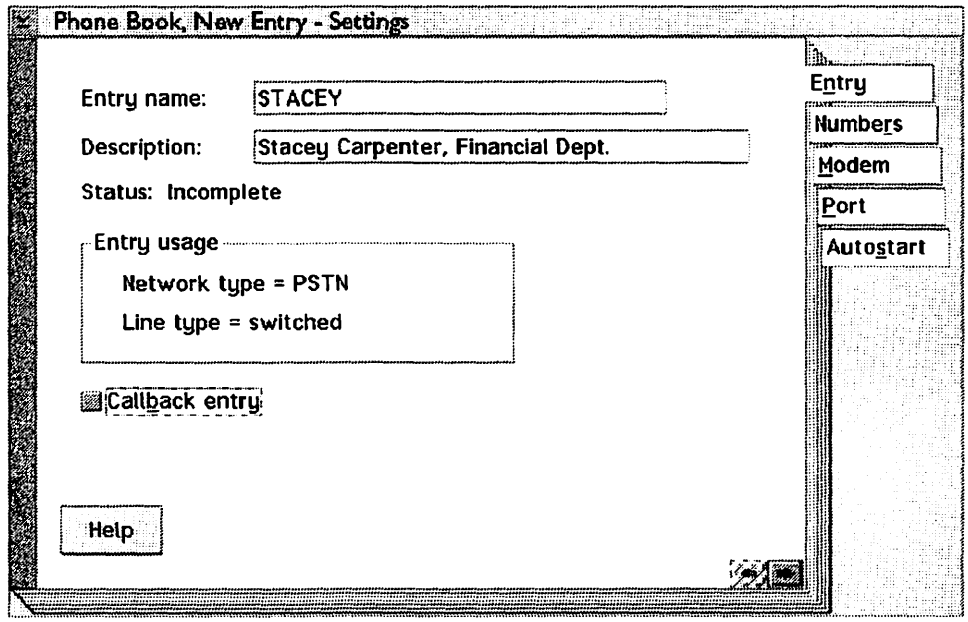


Figure 219. PhoneBook, New Entry - Setting Window (Entry Section)

Here you can add or change the PhoneBook entry name, the description and usage. This window also displays the status of the configuration.

5. Enter the **Entry name**.

   The Entry name field is used to specify the name of the workstation you dial. The entry name must be a unique entry in the PhoneBook.

   The field length is 15 characters.

6. Enter the **Description**

   The Description field is used to specify a description or notes about the workstation you dial.

7. Select the **Callback entry** check box.

   Note: The Entry usage area displays the type of network and line type you've configured for this PhoneBook entry.

8. Select the **Numbers** tab.

   A Phone number list box appears. The workstations you call might have more than one telephone number. You would use this list to view the telephone numbers of the PhoneBook entry and the order in which they are dialed. The top most numbers will be dialed first. To add a new number select the **Add...** button.

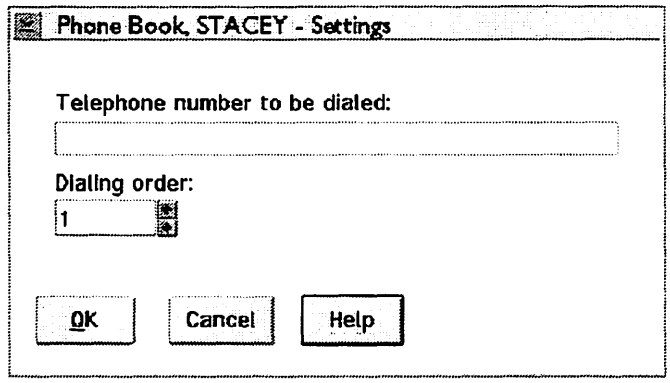


Figure 220. PhoneBook, New Entry - Settings Window

9. In the **Telephone number to be called** field, enter the phone number of the workstation you want to call. The field length is 32 characters.

   Note: The Dialing order field specifies the position of the telephone number in the PhoneBook entry call order list. The telephone numbers in the list are called from top to bottom. The top numbers are called first.

10. Select the **OK** button, which shows you the result. The number that you have added becomes part of the Phone number list box.

    Note: Use this list to add, change or delete telephone numbers. Use the appropriate push button to modify the telephone numbers, or the order in which they are dialed.

11. Select the **Modem** tab.

    The following window that is presented describes the modem capabilities of the workstation you are calling.

    A modem is either asynchronous or synchronous. If it is asynchronous, specify the class of the modem. If a modem is synchronous, specify the encoding scheme used to synchronize the transmittal of data.

    Based on the modem capabilities of the workstation you call, the software selects the correct modem on your workstation for the call.

    If the workstation you call has an asynchronous modem, an asynchronous modem is selected for your workstation that best matches the modem class of the modem on the workstation you call.

    If the workstation you call has a synchronous modem, a synchronous modem is selected for your workstation.

    If your workstation does not have an appropriate modem available, then the call will fail and a message will be displayed.

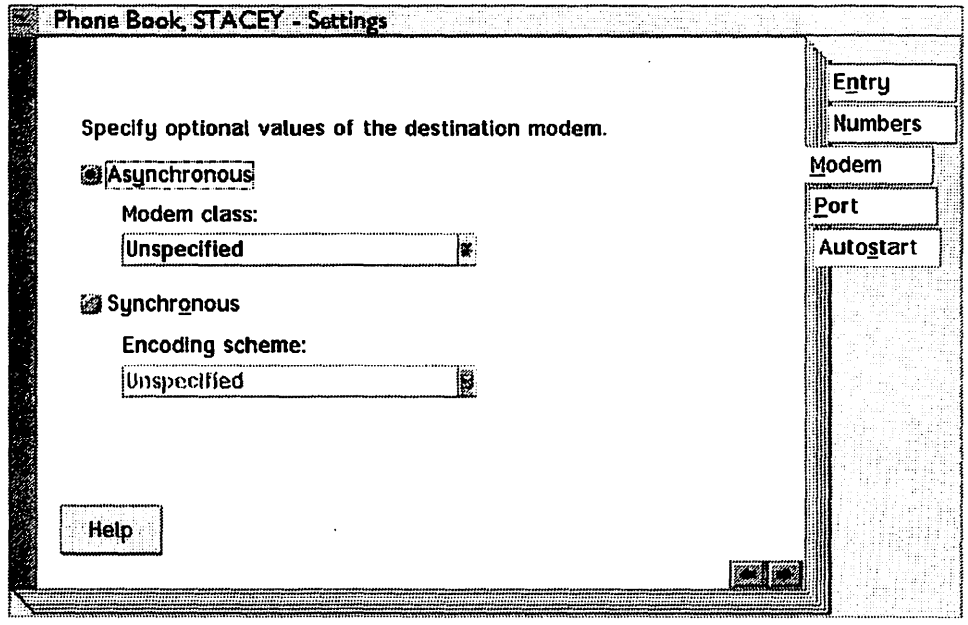


Figure 221. PhoneBook, New Entry - Settings Window (Modem Section)

This tab describes the modem capabilities of the workstation you are calling.

12. Select **Asynchronous**.

    Asynchronous is used if your external or internal modem uses the asynchronous data transmission mode.

13. Select the **Modem class**. This represents the fastest modulation standard supported by the asynchronous modem.

    Selecting a modem class is necessary only when you have multiple modems installed. If you have only one modem installed, the software uses the fastest modem class that is appropriate for your modem. Select a modem class for the workstation you are calling. The choices are:

    - Unspecified
    - V.22 at 1200 bps
    - V.22bis at 2400 bps
    - V.32 at 9600 bps
    - V.32bis at 14400 bps
    - Proprietary

    Note: The software selects one of your modems that best matches the modem of the workstation you are calling.

    Synchronous is used if your external or internal modem uses the synchronous data transmission mode. Consult your modem manual to select an encoding scheme for your synchronous modem. This parameter only needs to be defined for synchronous modems.

    The Encoding scheme parameter specifies the encoding scheme to be used when transmitting data for this call. The encoding schemes are:

    - NRZ
    - NRZI

14. Select the **Port** tab.

The following window is displayed. You use this tab if you have multiple ports and want to assign a specific port to a PhoneBook entry.

This tab is available only to workstations on a PSTN network with a switched line.

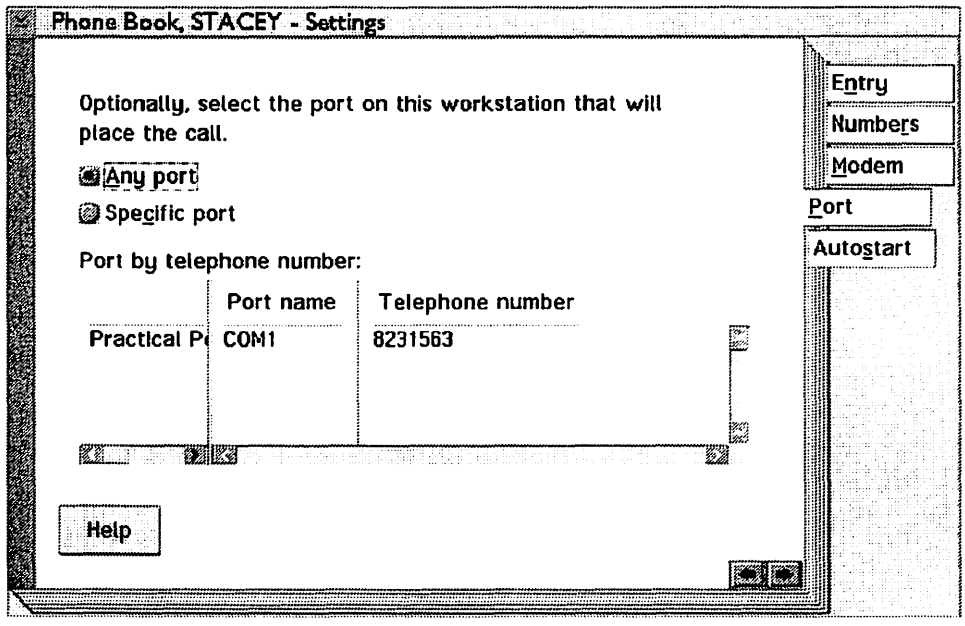


Figure 222. PhoneBook, New Entry - Settings Window (Port Section)

15. Select **Any port**.

    Any port is used if you have more than one port for your modems. Select **Any port** if it does not matter which port is used to call this PhoneBook entry.

    Note: Specific port is used if you have more than one port for your modems. Select it if you want to call this PhoneBook entry over a specific port and telephone number. You select the specific port and telephone number from the list under **Port by telephone number**. One scenario for using Specific port would be if you have certain modems that are supporting the same high speed protocol (and the other modems are not supporting this). Specifying the appropriate port would guarantee, for example in a callback enviroment, that the right modem calls back.

    A list is available only if you have multiple ports. If your workstation is configured for only one port, the associated phone number is automatically listed here.

    Port by telephone number lists the port name, the telephone number associated with the port, and the modem associated with the port.

16. Select the **Autostart** tab.

    The following window is displayed and is used to automatically start a LAN-based program with the workstation you call. The LAN-based program is started when you establish a connection.

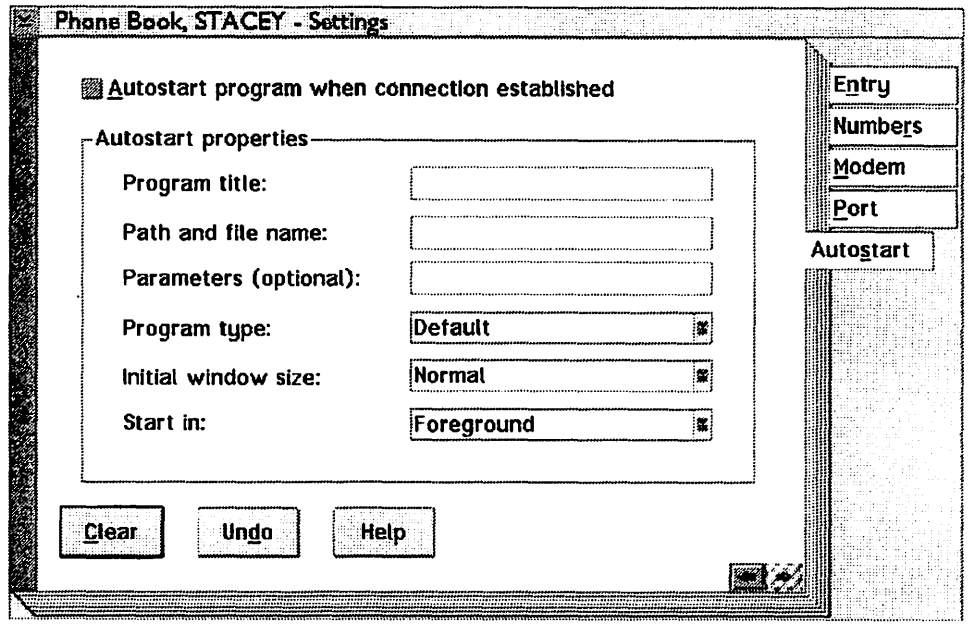


Figure 223. PhoneBook, New Entry - Settings Window (Autostart Section)

Note: In our example we don't configure that window.

17. Close the **PhoneBook, New Entry - Settings** window.

That brings you back to the Settings window shown in Figure 224.

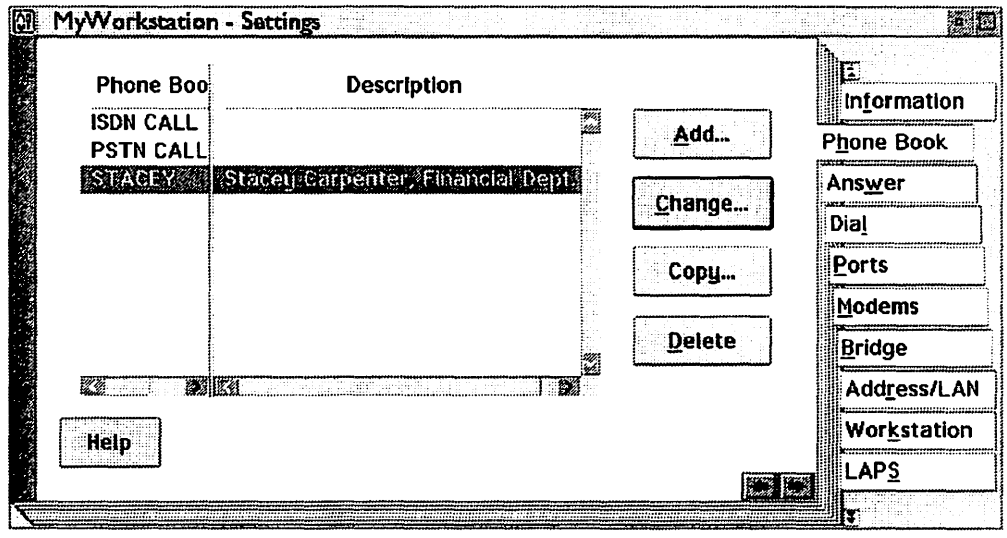


Figure 224. Settings Window

Here you can see that the user we configured before is now in the PhoneBook list.

Modifying MPTS for Remote Access Services Installation

The Remote Access Services installation process adds both the Remote Access Services Logical Adapter for the WAN connection and the real network adapter in LAN Adapter and Protocol Support (LAPS). In order to use Remote Access Services with other protocols or when you want to change parameters, you must open the LAPS configuration.

To configure LAPS do the following steps:

Note: To see and select the LAPS tab you must first use the scroll-down tab or maximize the window.

1. From the Settings notebook select the **LAPS** tab.
2. Select the **LAPS...** button to start the LAPS configuration.

   You now see the MPTS Configuration window as shown in Figure 225. You can see that in the Current Configuration section, the LAN Distance Logical Adapter with NetBIOS and the network adapter is installed. This is where you can make changes or add adapters and protocols.

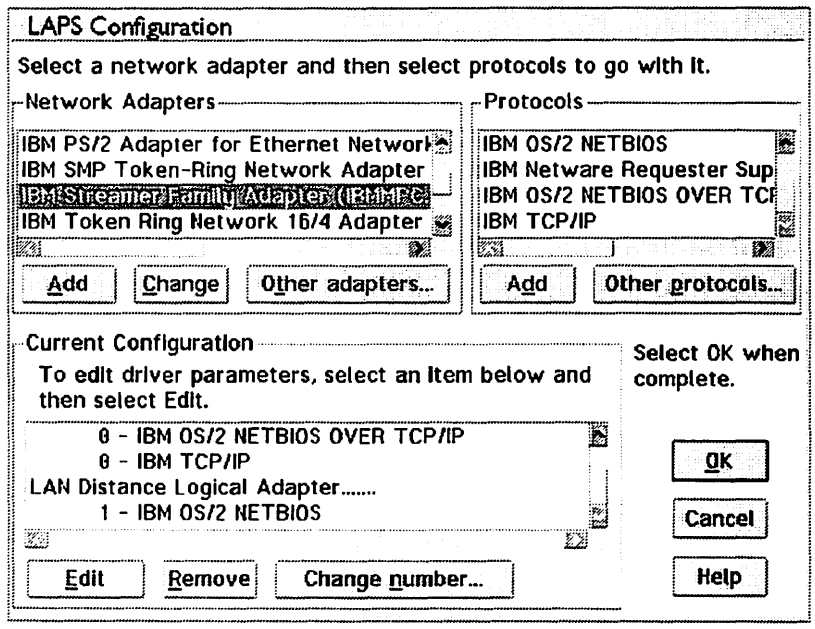


Figure 225. LAPS Configure Workstation Window

NetBIOS Requirement

NetBIOS is required by Remote Access Services for security and system management functions. *If you delete NetBIOS, Remote Access Services will not work* (even if you have security disabled).

3. Select the **OK** button to finish the LAPS configuration.

Save the Configuration and Restart the Workstation

Remote Access Services should now be fully configured and ready to accept incoming calls from remote workstations to the local LAN. Remote Access Services must be shut down and the workstation restarted for the changes to take effect.

1. Close the **MyWorkstation - Settings** notebook window.

   You receive a message asking you if you want to save the **Settings** notebook values.

2. Select **Yes**.

   You receive a message telling you that some changes to the Settings notebook require you to stop and restart Remote Access Services. Other changes require you to shut down and restart the workstation.

You can select the **Help** button to see what configuration changes require you to simply stop and restart Remote Access Services, and what configuration changes require the workstation to be restarted.

3. Select the **OK** button.
4. Stop all your running programs.
5. Shut down your system from the OS/2 Desktop.
6. Restart your workstation (Ctrl-Alt-Del).
7. Start the Remote Access Services program from the within the IBM Remote Access Folder. Ensure that your modem is connected and powered on before you start the Connection Server.

   You may wish to copy the Remote Access Services icon into the OS/2 Startup folder, so that Remote Access Services is started each time you start the workstation.

   The Connection Server is now installed and ready for operation.

7.5 Setting Up an OS/2 Remote Access Services Client

OS/2 Warp Server includes client software. Part of this client software is the Remote Access Services client software. The Remote Access Services client software is the IBM LAN Distance Remote for OS/2 software. This software is also available within OS/2 Warp Connect or can be purchased separately.

Installation Considerations

In this section we will describe the installation of the Remote Access Services client. There are two options available for installing this software. They are:

1. Using the Client Installation program - Advanced Path
2. Installing using a redirected drive or off diskettes

Integrated Client Installation

This procedure would normally be used when you set up a new machine. The procedure uses a redirected drive to allow you to install an OS/2 Client with a number of options. One of these options is to install the Remote Access Client. When you install an OS/2 Client you will be presented with the panel as shown in Figure 226 on page 314

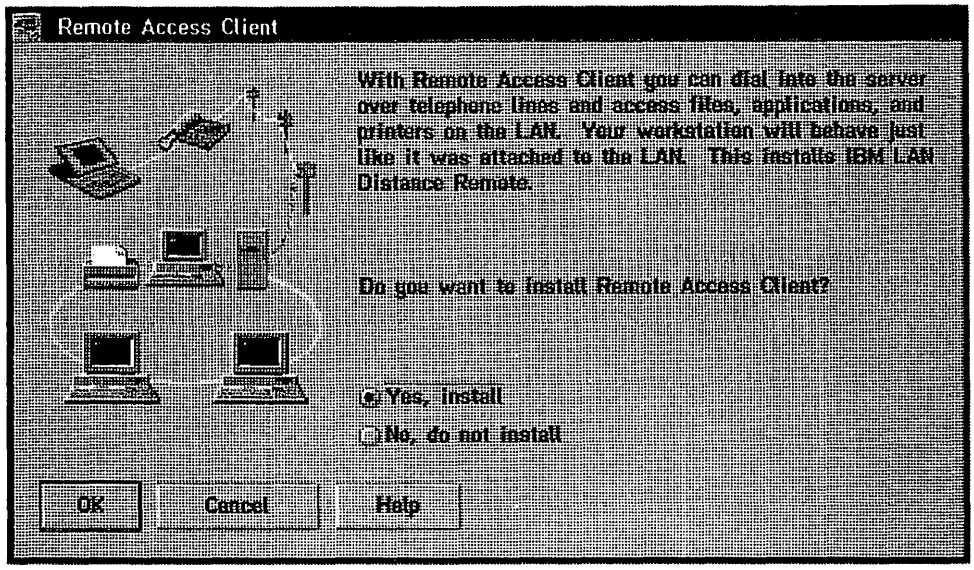

Remote Access Client
With Remote Access Client you can dial into the server over telephone lines and access files, applications, and printers on the LAN. Your workstation will behave just like it was attached to the LAN. This installs IBM LAN Distance Remote.
Do you want to install Remote Access Client?
Yes, install
No, do not install
OK
Cancel
Help

Figure 226. Remote Access Client Selection

If you choose **yes** on the preceding panel you will be prompted for the parameters as shown in Figure 227.

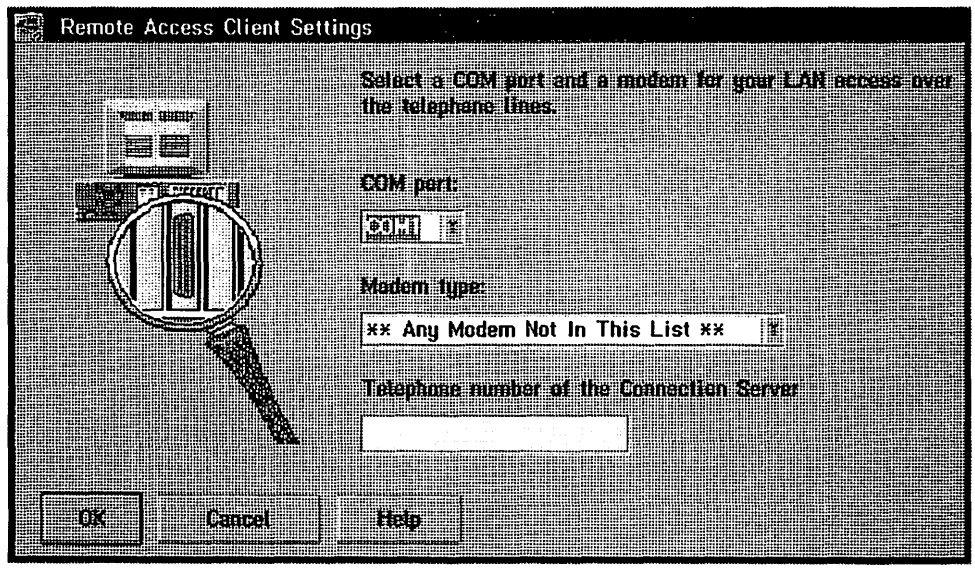

Remote Access Client Settings
Select a COM port and a modem for your LAN access over the telephone lines.
COM port:
Modem type:
** Any Modem Not In This List **
Telephone number of the Connection Server
OK
Cancel
Help

Figure 227. Remote Access Client Selection

There are a number of points which should be considered when completing this panel:

- **Telephone number of the Connection Server**

  This field is optional. The telephone number entered here will appear as the default entry when you first open your Phone Book in order to make a connection. However, additional entries can be made in the Phone Book, at the workstation, after the installation has completed.

  In this case, enter the telephone number, of the connection, you will be calling most frequently.

- **Modem**

If you are going to be making an asynchronous or synchronous, switched or leased connection, choose the appropriate modem from this list. If the modem that you wish to use does not appear on the list, it is possible that selecting one of the other modems (a similar type or generic Asynchronous Switched Modem) will work.

Alternatively, you will need to install a modem PIF (Product Information File) file at the workstation, after the installation has completed. A modem PIF file is simply installed by copying the file into the x:\WAL directory on the workstation. The workstation will then need to be configured at the workstation using the LAN Distance Settings Notebook. PIF files can often be obtained from your modem manufacturer, but it is also possible to create your own using CFMODEM, a utility that is supplied on the OS/2 Warp Server CD-ROM.

For further details on using CFMODEM, please refer to 7.14, "PIF Files for Uncertified Modems" on page 363. For more information on configuring the client from the Settings Notebook, please refer to the online Help.

- **COM Port**

  The integrated installation requires that you select a COM Port to validate installation.

  If you wish to use another connection type, such as ISDN, you will need to configure this at the workstation from the LAN Distance Settings Notebook after the integrated installation has completed. For further information on configuring an ISDN connection, please refer to the online *LAN Distance Requester Guide*.

  There is a file giving further detail on configuring and using Remote Access Services over an X.25 PAD connection supplied with OS/2 Warp Server This file, X25RME.ZIP, is in compressed format on CDROM1 and should be expanded, using the PKUNZIP2 utility, onto your hard disk with the following command:

  ```
  x:\IBMCOM\PKUNZIP2  y:\CID\IMG\LDR\L0265R3\WAL\X25RME.ZIP  z:\TEMP
  ```

  Where x: is the drive containing your IBMCOM subdirectory, y: is your CD-ROM drive (which may be a redirected drive across the LAN) and z:\TEMP is the directory in which you wish to place the uncompressed readme file.

Manual Remote Access Client Installation

You would use this method when you are installing a workstation whose existing software configuration you wish to keep. With this installation you can install just the remote access code and leave existing software alone.

The Remote Access Services client can also be installed off a redirected drive, directly off the OS/2 Warp Server CD-ROM or manually created diskettes. The diskette images are stored on the CD-ROM in the drive:

```
x:\CID\CLIENT\LDREM\IMAGES\OS2
```

The considerations in "Integrated Client Installation" on page 313 also apply to this installation procedure. Please refer to the *IBM LAN Distance Requester Guide* if you need further information.

Shuttling between LAN-Attached and Remote Workstation Configurations

The Shuttle option allows you to use your workstation and its applications in either the LAN-attached or the remotely attached environment. To use this option, you must have a LAN adapter installed in your workstation and a working LAN-attached configuration.

Shuttling between the LAN-attached and remote environments can be accomplished by:

- Typing LDSHUTTL at an OS/2 command prompt and pressing Enter
- Starting LAN Distance when the machine is configured as a LAN workstation
- Closing the LAN Distance container on a workstation that is set up to operate as a Remote Workstation

Figure 228 shows the Shuttle Option window.

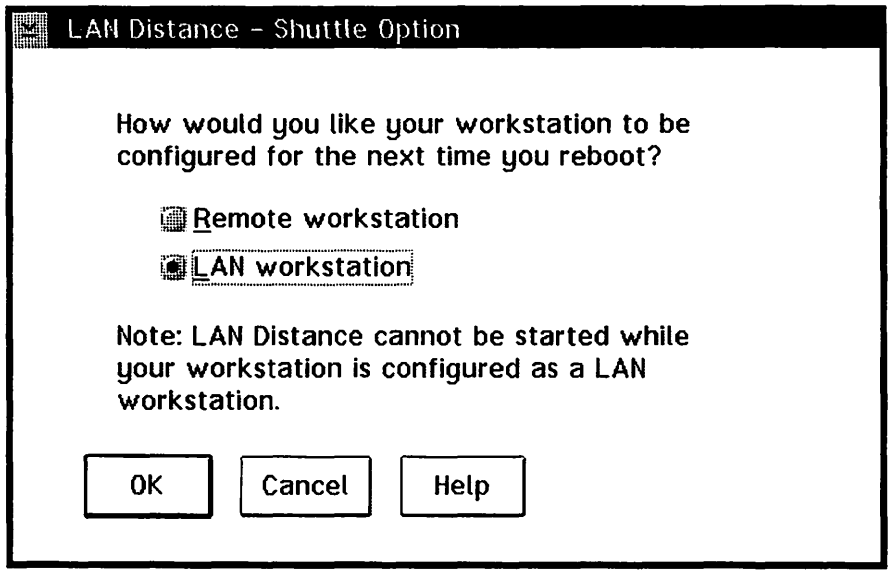

LAN Distance - Shuttle Option
How would you like your workstation to be configured for the next time you reboot?
Remote workstation
LAN workstation
Note: LAN Distance cannot be started while your workstation is configured as a LAN workstation.
OK
Cancel
Help

Figure 228. Shuttle Option Window

1. Select how you want the workstation to be configured after the next reboot, **Remote workstation** or **LAN workstation**.
2. Select **OK**.
3. Shut down and restart (Ctrl-Alt-Del) your workstation to activate the new configuration.

The Shuttle feature provides an easy mechanism for switching the machine between the two types of workstation configuration at any time. When you have just completed the installation from the OS/2 Warp Server CD-ROM, your workstation will be in LAN mode. You must run the shuttle function if you wish to use the workstation as a Remote workstation.

Note: The Shuttle feature changes both your CONFIG.SYS and PROTOCOL.INI files. LAN Distance handles two different PROTOCOL.INI files. One for LAN connection and one for remote connection. One of these files is in active use, and the other one is backed up. Shuttle switches between these two files. After Shuttle changes the PROTOCOL.INI file, the CONFIG.SYS file is edited to support

the device driver statements required for the current PROTOCOL.INI. This means that any changes in the MPTS configuration (stored in PROTOCOL.INI) only affect the currently active configuration.

For example, if you install an application that changes PROTOCOL.INI while your workstation is attached to the LAN, that change is not automatically made in the other PROTOCOL.INI used when the workstation is a Remote Workstation. To run that application on the Remote Workstation, you would need to use MPTS to update the PROTOCOL.INI with the appropriate changes.

Order of Installation

Because of this potential problem of having your PROTOCOL.INI files not properly updated, it is recommended that Remote Access Services always be installed *after* all other network applications on your workstation. Install the network applications and verify that they are working correctly on the real LAN before installing Remote Access Services.

If you already have installed Remote Access Services, and you require to install another network application (one which will make changes to your PROTOCOL.INI file), the safest way to do this is to remove Remote Access Services, using the LDREMOVE command, install the network application, then reinstall Remote Access Services.

7.6 Setting Up a Windows Remote Access Services Client

OS/2 Warp Server includes the Windows client software. The Remote Access Services client software is the IBM LAN Distance Remote for Windows software. This software can also be purchased separately.

In this section we will give a very brief overview of the installation. For detailed information refer to the documentation referenced at the end of this chapter.

Limitations

The following features are not supported, or are not fully supported for the MS Windows version:

- Administrative tools, such as Audit, and Call and Port Management, are not supported in the MS Windows version.
- Local security is not supported on the MS Windows workstations.
- LAN Distance Remote for MS Windows supports an asynchronous COM port connection. ISDN and synchronous connections are not supported for MS Windows workstations.
- Only one asynchronous COM port connection (COM1 through COM4) is supported for LAN Distance Remote MS Windows workstations. Multiport configuration and ARTIC multiport adapters are not supported for MS Windows workstations.
- Setting up a LAN Distance Remote MS Windows workstation to answer calls is different from setting up a LAN Distance Remote OS/2 workstation.
- Serial device support is automatically loaded for MS Windows workstations. MS Windows detects the existence of up to four COM ports on your LAN

Distance MS Windows workstation, but cannot guarantee whether these ports are in use.

- Installation using diskettes is supported for LAN Distance Remote for MS Windows. Redirected drive installation using the LDIMAGE program and response file installation is not supported for MS Windows workstations.

  The error message file, WALINST.LOG, is not accessible for LAN Distance Remote MS Windows workstations.

- The LDREMOVE utility used to remove the LAN Distance Remote for MS Windows files does not archive your LAN Distance user configuration files.
- The LAN Distance Remote for MS Windows product does not supply or install all LAN networking software. Use LSP(LAN Support Program) to run 802.2 applications on your stand-alone LAN Distance Remote. If you plan to shuttle to the LAN-attached environment, use LSP to install the necessary LAN protocols for your LAN applications.
- The Shuttle feature for LAN Distance Remote for MS Windows is installed as an icon in the LAN Distance container, and can be invoked by double-clicking on this icon.

Installation Considerations

In this section we will describe the installation of the Remote Access Services client. There are two options available for installing this software. They are:

1. Using the Client Installation program - Advanced Path
2. Installing using diskettes

The diskette images for the windows client are on the OS/2 Warp Server CD-ROM in the following directory:

```
x:\CID\CLIENT\LDREM\IMAGES\WIN
```

Once you have created the diskettes you can do a manual installation at the client by inserting the first diskette and initiating the installation program. The installation program is the same as the integrated installation program described in the next section.

Integrated Client Installation

This procedure would normally be used when you set up a new machine. The procedure uses a redirected drive to allow you to install the Windows Client options. One of these options is to install the Remote Access Client.

As part of the integrated installation you can select to install the Remote Access Services client. You will be prompted for the installation drive. At this point all the files are transferred to the selected drive. You then have the option of going through the Basic Settings or to reboot and configure the Remote Access Services through the LAN Distance Notebook. The Basic settings should be sufficient for most installations. Should you choose to configure the client through the Basic Settings you will be prompted for the following information:

- **Modem**

  If you are going to be making an asynchronous or synchronous, switched or leased connection, choose the appropriate modem from this list. If the modem that you wish to use does not appear on the list, it is possible that selecting one of the other modems (a similar type or generic Asynchronous Switched Modem) will work.

Alternatively, you will need to install a modem PIF (Product Information File) file at the workstation, after the installation has completed.

- **COM Port**

  The integrated installation requires that you select a COM Port to validate installation.

  If you wish to use another connection type, such as ISDN, you will need to configure this at the workstation from the LAN Distance Settings Notebook after the integrated installation has completed.

- **Telephone number of the Connection Server**

  This field is optional. The telephone number entered here will appear as the default entry when you first open your Phone Book in order to make a connection. However, additional entries can be made in the Phone Book, at the workstation, after the installation has completed.

  In this case, enter the telephone number of the connection you will be making most frequently.

- **LAN Type**

  In this field you can select either Token Ring or Ethernet. The LAN type is dependent on the network that your connection server is connected to.

- **Adapter Number**

  You have to define a LAA (locally administered address) for your remote workstation. As its name suggest, this address should be given to you by your local LAN administrator, because it has to be unique on the LAN. Should two workstations have the same LAA, only the first one trying to connect would succeed. The second address would be rejected.

- **NetWare Requester Support**

  If you choose to enable the NetWare DOS/Windows client, you then have to specify the directory containing your NetWare client code. Usually this is C:\NWCLIENT.

  If you did enable NetWare support, you have to specify the type of frame. This should correspond to the frame type defined on your NetWare server. Ask your network administrator for this frame specification.

Once the installation has completed you can choose to reboot either as a remote or as a local workstation. Your remote workstation is now ready to dial into the connection server.

An icon is included in the LAN Distance program group that performs the shuttle feature.

7.7 Mobile File Sync and Remote Access Services

Mobile File Sync (MFS) is a file system that supports mobile OS/2 Warp clients. Mobile File Sync allows users to physically disconnect from the LAN Server 4.0 or Windows NT server and still have access to their server files. Warp clients can be either LAN Requester clients or OS/2 Peer clients. MFS is available as part of the OS/2 Warp Attachpak.

Mobile File Sync caches the accessed files and directories to the client machine. When the client is disconnected from the server, the user can continue

accessing the files and directories previously cached from the server. The user can read the cached files, update them, or create new files. The user can also list contents of cached directories, create new directories, or delete existing ones. Mobile File Sync keeps track of all updates by recording them in a "Client Modification Log." All updates are propagated to the server, when a new connection is established, in a process called *Reintegration*.

MFS can be used on its own or together with Remote Access Services for LAN Distance.

MFS Functions

Mobile File Sync provides the user with three levels of functions:

- Basic

  This level includes implicit caching and reintegration. Mobile File Sync (MFS) users automatically get the benefit of implicit caching. Assume that the user accesses server name S, and maps the D: drive and S to the local M: drive. Files and directories on the M: drive can now be accessed for reading or updating. Accessed files and directories will be automatically cached on the client machine. No specific action is required by the user to activate the implicit caching.

- Intermediate

  This level includes explicit caching using the *Stash* feature. In some cases the user knows that he will need some files while he is disconnected from the server, but does not want to explicitly access those files. The stashing mechanism provides this function. The user can use stashing to ensure that needed files exist on the client before a planned disconnection.

- Advanced

  This level includes the *Spy* utility. The *Spy* utility allows a user to monitor Mobile File Sync activities in order to find out what files are actually being accessed by the application. Those files can then be inserted into the Stashing Database and brought into the user's cache.

Once you have installed MFS, you need to configure the level of function that you are going to use. No further configuration is required for basic functionality. Further details on using MFS is available in the online documentation.

Using MFS with Remote Access Services

Remote Access Services provides a level of transparency to applications. Applications are not really aware of their state of attachment. Although the link is remote, for all intensive purposes the application considers the link to be local. The same applies to MFS. MFS is not aware of the state of the machine, that is, local or remote, it only checks for a link to a drive as being active or inactive.

Advantages of this are, if you have a slow or bad connection you could use MFS to work on the file and only connect to the connection server to perform the updates. MFS allows you the flexibility to work on data even when you do not have access to a connection. The reintegration process can then proceed unattended when you reestablish the connection.

Irrespective of the level of function that you use with MFS they all operate in a similar way during the process of reintegration. MFS caches files and offers the user the same drive letter that they used while connected to the network. For example, a user that caches drive M on the network to access data files for a spreadsheet application will have drive M still available once he has disconnected from the network. All cached files will still be available.

At this point MFS is in a state of connected. This is shown by the MFS icon on the desktop , MFS Status M:CONN.

Once the user disconnects from the network MFS is in a state of disconnected. This is indicated by MFS Status M:DISC. The user can continue working on the file even though they are disconnected. The file they are accessing is cached on the local hard drive.

Once the user reconnects to the network either by locally attaching their machine or by dialing in using Remote Access Services MFS goes into a status of reintegration. MFS Status M:REINT. During this process no files on the matched drive should be modified until reintegration is completed. The status icon will be MFS Status M:CONN once the integration is done.

Considerations

The following should be taken into account when using MFS and Remote Access Services:

Updates

Because you could be working on a *copy* of a file the possibility of the file being updated while you are disconnected is a reality. Although you will be warned by MFS you should consider only using MFS to work on files that are either not shared or cache files that need to be shared but are seldom updated.

Time-Outs

There are a number of parameters that determine whether the connection to the server is available or not. Also when a session is timed out. These have been explained in previous sections.

The Mobile File Sync program uses a dynamic time-out strategy. Low level file system requests that can be completed in 15 seconds to 60 seconds are handled automatically.

Although a large file may take several minutes to update over the phone line it will not timeout because the transfer is composed of many smaller reads and writes. The timeout values apply to the small reads and writes and not the complete file transfer. The strategy also compensates for periods of time when network traffic is very high and response is slow, and dynamically adjusts to the response speed of various communications media.

You can change the timeout management if the file system requests are expected to be less than the minimum value of 15 seconds, or longer than the maximum value of 60 seconds. The minimum value and maximum value can be specified in CONFIG.SYS as follows:

```
MFSMINTIMEOUT=x,  x is the minimum number of seconds before time-out.
MFSMAXTIMEOUT=y,  y is the maximum number of seconds before time-out.
```

One or both may be specified. The value for x and y must be an integer between 1 and 65,536. X and y can have differing values, but the value for MFSMINTIMEOUT must be less than or equal to the value for MFSMAXTIMEOUT.

The defaults should be sufficient for most situations.

Cached Files

MFS is meant to serve as a file caching utility to cache files that are may be updated and require automatic synchronization. For this reason it is best to cache data files rather than applications. Because applications are usually large and will not change it is best to store applications on the hard drive of the mobile machine.

To ensure that application files are not cached ensure the drive that you are caching does not contain application files that may be accessed by you during the connected session.

Cache

MFS allows you to set limits on the amount of disk space that it can use for caching files and on the number of files that it can cache. These limits are set with the following environment variables in CONFIG.SYS:

- `MFSCACHESIZE=x`

  Where x can be any integer in the range of 10 to 50. If MFSCACHESIZE is not defined in CONFIG.SYS, a default value of 10 is used.

  This is an upper limit on the disk space that can be used by MFS for caching. This is specified as a percentage of the free space available on the cache drive and can be in the range of 10%-50% of the free space on the cache drive. The cache drive is the drive on which the MFS cache resides, and can be determined from the environment variable MFSCACHE in CONFIG.SYS. For example, if CONFIG.SYS contains the line: `MFSCACHE=D:\MFS\CACHE`, then the cache drive is `D:`.

- `MFSMAXFILES=x`

  Where x is any integer in the range of 1,024 to 65,536. The default value is 1024.

  This sets a limit on the number of files that can be cached by MFS

7.8 Deinstallation

To remove the Remote Access Services or the Remote Access Services client programs you need to run the the LDREMOVE program. This program may also be used if you have had a partial install or deinstall of the Remote Access Services components. This procedure may be used on both client and server machines:

1. From an OS/2 command line, type `LDREMOVE`.

   If the LDREMOVE program is not found, insert the product diskette 1 in the diskette drive, type

   ```
   A:\LDREMOVE
   ```

   and press Enter. If the LDREMOVE program is found, the Remove LAN Distance window is displayed. Continue to step 3. If the LDREMOVE

program is not found, the REXX program needed to run the LDREMOVE program may not be installed on your workstation, go to step 2.

2. Try using the LDREM command, which does not require the REXX program. With Diskette 1 in the diskette drive, from an OS/2 command prompt, type

   x:\LDREM

3. From the Remove LAN Distance window, specify whether you want to archive or delete LAN Distance configuration files.
   - Select the Delete configuration files radio button to remove LAN Distance configuration files.
   - Select the Archive configuration files radio button to store a backup copy of your LAN Distance configuration files.

     The user configuration files listed in LAN Distance User Configuration Files are stored in the WAL\BACKUP directory. User configuration files are not automatically restored when you install the LAN Distance Connection Server program again. To restore the information in these files, manually copy the files after you install the Remote Access Services server or requester.
4. Select the **Remove** push button to start the removal process.
5. When the Remove Complete window appears stating that removal is complete, shut down and restart your workstation.

All the Remote Access Services code will now be removed from workstation, with the exception of the following files, which are stored in the \WAL\BACKUP subdirectory.

CONFIG.WAL	Copy of last Remote CONFIG.SYS
PROTOCOL.XXX	PROTOCOL.INI files used for switching LAN to Remote configurations
WCBUSRF.ISF	Security account database
WCLDIAL.CXD	Phonebook entries
WCLLOCAL.INI	Workstation-specific configuration file
WCLNET.INI	Modem configuration file

7.9 Inactivity Timeout Feature

One of the new features that the Remote Access Services introduces over existing LAN Distance connection servers is the inactivity timeout feature. This feature is available on both Connection Servers and Remote OS/2 workstations. When enabled this feature subjects every machine that connects to it to a usage test every minute. The usage test checks how many LAN frames have passed across a link and depending on the values set decides whether the link should remain up or disconnected.

Figure 229 on page 324 shows the Shuttle Option window.

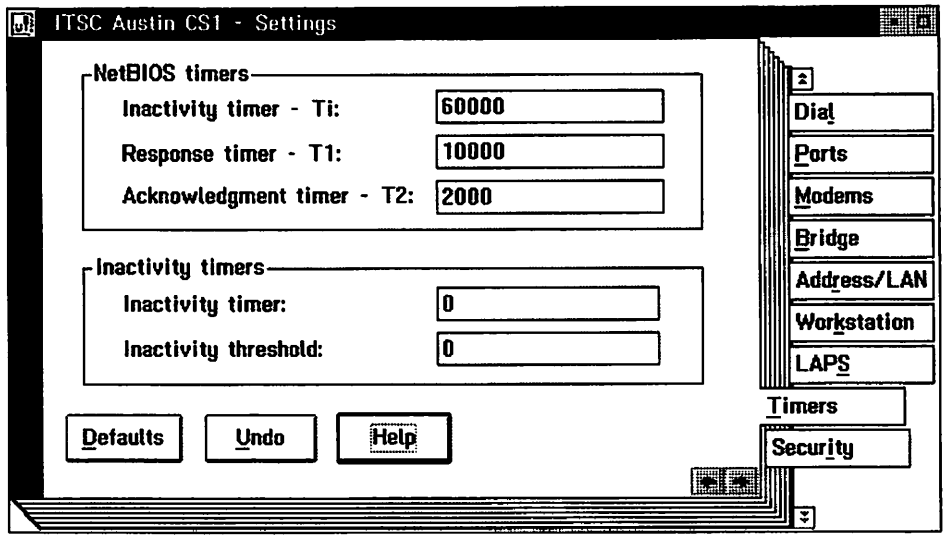


Figure 229. Inactivity Timeout Option

Figure 229 shows the timers Notebook page where the Inactivity timeout is set. Two values need to be set:

1. **Inactivity timer**

   This timer specifies the maximum amount of time in minutes to allow idle activity before the connection is disconnected. The default value of 0 disables the inactivity timeout function. The range of the value is between 0 and 999.

2. **Inactivity Threshold**

   This timer specifies the minimum number of frames required to cross the WAN link on an active connection within one minute. If the number of frames per minute falls below this timer value for the length of time specified in *Inactivity timer* the connection will be disconnected.

   The default value of 0 disables the inactivity timeout function. The range of the value is between 0 and 99999.

7.10 Adding Multiple Lines to the Remote Access Services

This section covers the configuration changes required to support multiple asynchronous lines on the Connection Server, using standard COM ports. You need to complete the following steps to add additional lines to the Connection Server:

- Install and configure the necessary adapter hardware
- Use the Settings Notebook to:
  - Configure the additional WAN Ports
  - Configure the attached Modems

In the ITSO test environment we installed the IBM Dual Asynchronous adapter to equip the Connection Server with two more ports.

Following the steps below to configure the Connection Server to support multiple asynchronous lines.

Open the Remote Access Services Settings Notebook

1. Open the IBM Remote Access icon by double clicking on it. This icon is contained within the LAN Distance Remote Access folder.
2. If you have multiple Connection Servers on your network choose the one you are configuring.
3. Select **Selected** from the menu bar.
4. Select **Open as →**.
5. Select **Settings**.

You have now opened the Settings notebook and are ready to start the configuration.

With multiple asynchronous lines, one modem is attached to each of the COM ports. You have to configure which modem each of these ports will use.

In this example, we installed an IBM Dual Asynchronous adapter in the Connection Server. It has two COM ports that should be configured, as follows:

1. Select the **Ports** tab.

   The following window is displayed, where you find a list of the ports that are already configured. In this example, only one COM port with an asynchronous adapter is configured.

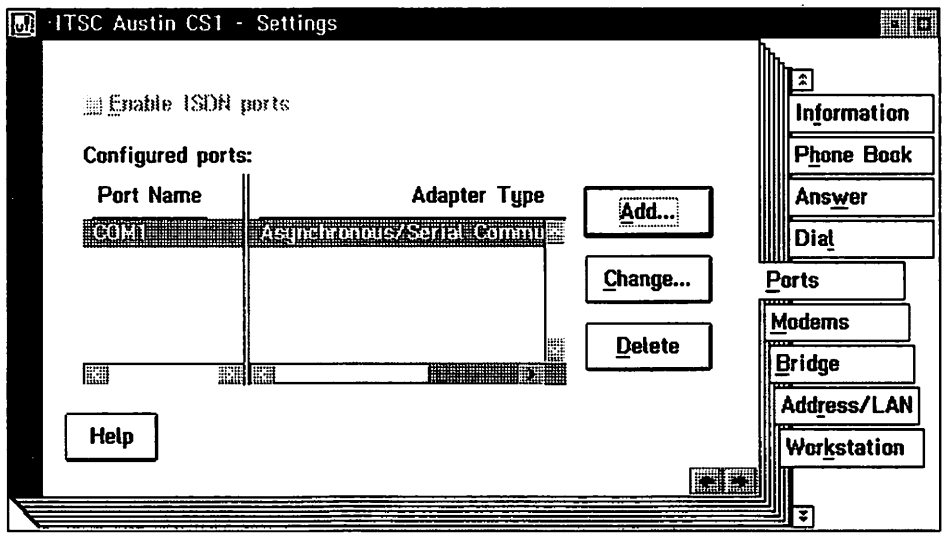


Figure 230. Settings Notebook, Ports Tab

2. Select the **Add** button.

   The following window is displayed, and you can select the type of adapter for the port.

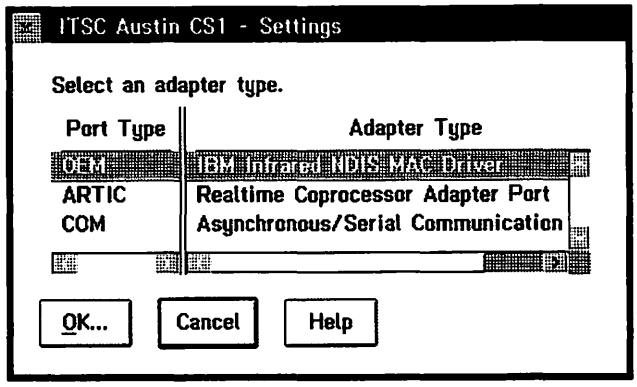


Figure 231. Adapter Type Selection Window

3. Select **COM** as the Port Type in order to configure the asynchronous communications ports.
4. Select the **OK** button.
5. In the Asynchronous/Serial Communication Ports - Settings window, select the COM port you want to configure.
6. You have the option to specify a new title for this port in the Port title field.
7. Select whether this port uses a *Switched* or *Nonswitched* line type.
8. Leave the rest of the fields blank to accept default values. The default values are tuned for the product.
9. Close the window.

   This port is now added to the Configured ports list, as shown here:

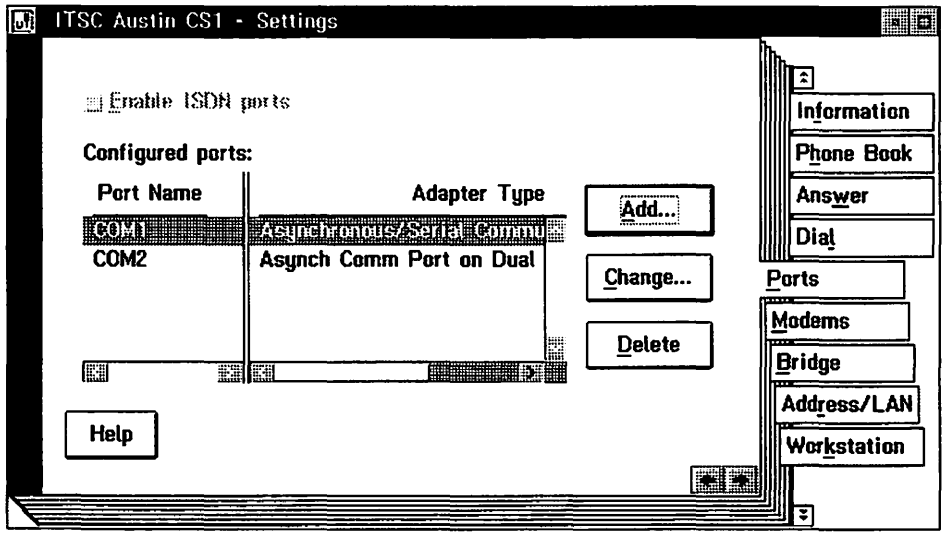


Figure 232. Settings Notebook, Ports Tab

10. Select the **Add** button again if you want to add more ports.

After all ports are added, you have to configure the modem for each port.

Configure the Modems

1. Select the **Modems** tab in the Settings notebook.

   The following window is displayed:

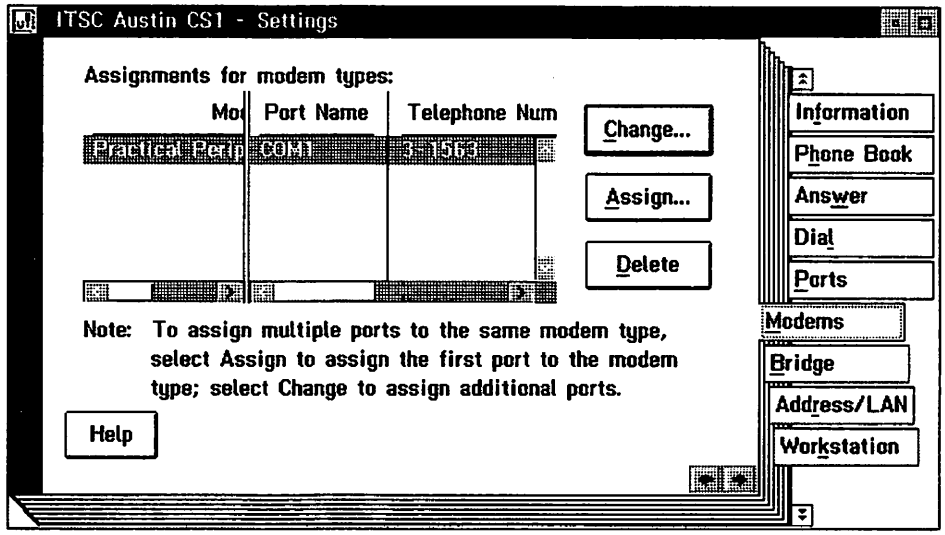


Figure 233. Settings Notebook, Modems Tab

   In the Modem type assignment field of the Assignments for modem types window, you can see the what modem type the Remote Access Services already is configured for.

2. If you are assigning multiple ports to the modem type that is already being used, then select the **Change** button. Select the **Assign** button to select a new modem type.

   - If **Assign** is selected, then the Select Modem window in Figure 233 is displayed. Continue with the next step.
   - If **Change** is selected, the Ports currently assigned window is displayed as shown in Figure 234 on page 328, and you can go to step 5. Be aware that you should have the same Universal Asynchronous Receiver/Transmitter (UART) type for any COM port that you are adding to a previously set up modem type. Otherwise, you may have to change the port speed, in the modem initialization file. For example, if the speed was set up for a FIFO COM port but the COM port you are adding is non-FIFO, which is a different UART type, you need to lower the port speed or you will receive an error message each time you start the Connection Server. You can use the CFMODEM utility to change the port speed. For more information, see discussions in 7.14, "PIF Files for Uncertified Modems" on page 363.

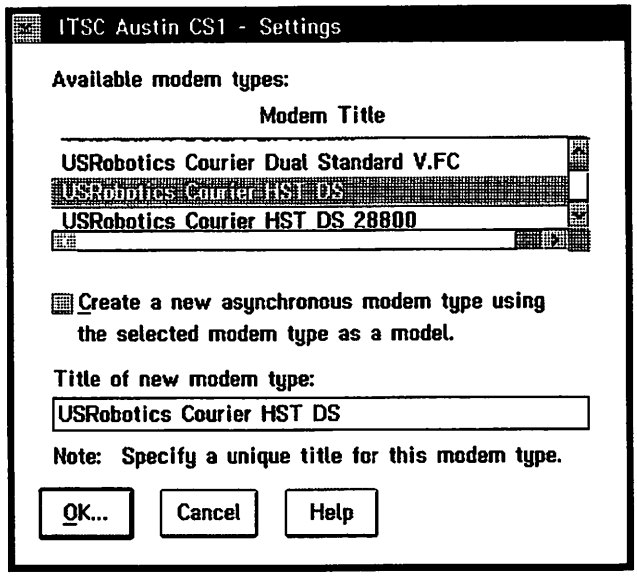

ITSC Austin CS1 - Settings
Available modem types:
Modem Title
USRobotics Courier Dual Standard V.FC
USRobotics Courier HST DS
USRobotics Courier HST DS 28800
Create a new asynchronous modem type using the selected modem type as a model.
Title of new modem type:
USRobotics Courier HST DS
Note: Specify a unique title for this modem type.
OK...
Cancel
Help

Figure 234. Select Modem Window

3. Select a modem from the Available modem types list.

   Note: If your modem is not among the listed modems, you should read 7.14, "PIF Files for Uncertified Modems" on page 363 in order to set up your specific modem.

4. Select the **OK** button.

   Now the window where you assign ports to the selected modem type, as shown in Figure 235, is displayed.

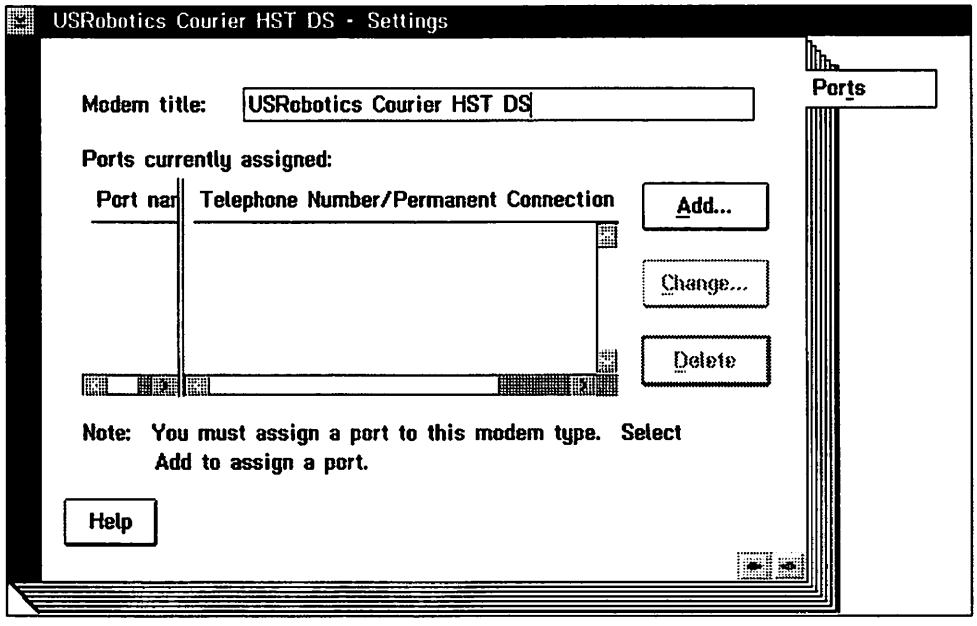


Figure 235. Ports Currently Assigned Window

The Modem title field shows the modem type selected in the previous window.

The Ports currently assigned field shows the COM ports that are configured to use the selected modem type. If no port is configured for this modem type, then the list is empty as in this example.

5. Select the **Add** button to add ports to the Ports currently assigned list for the modem.

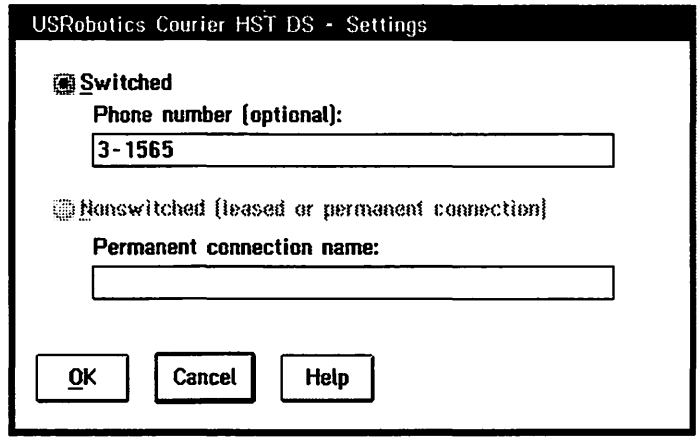


Figure 236. Phone Number Window

6. Enter the Phone number to be dialed by a Remote Workstation in order to connect to the Connection Server via this modem and port. (It is optional to configure this. You should fill this field for later use with call and port management).
7. Select the **OK** button.

   Next, the **Available ports** list in Figure 237 is displayed.

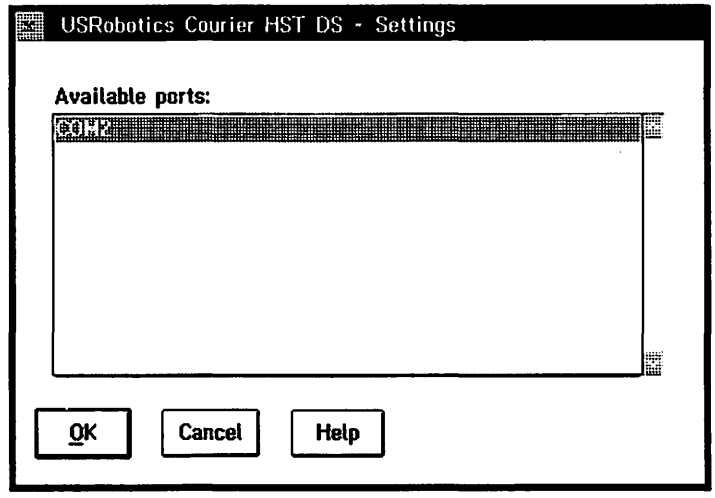


Figure 237. Available Ports Window

8. Select one of the available ports.
9. Select the **OK** button.

   Now the Ports currently assigned list in Figure 238 on page 330 is displayed.

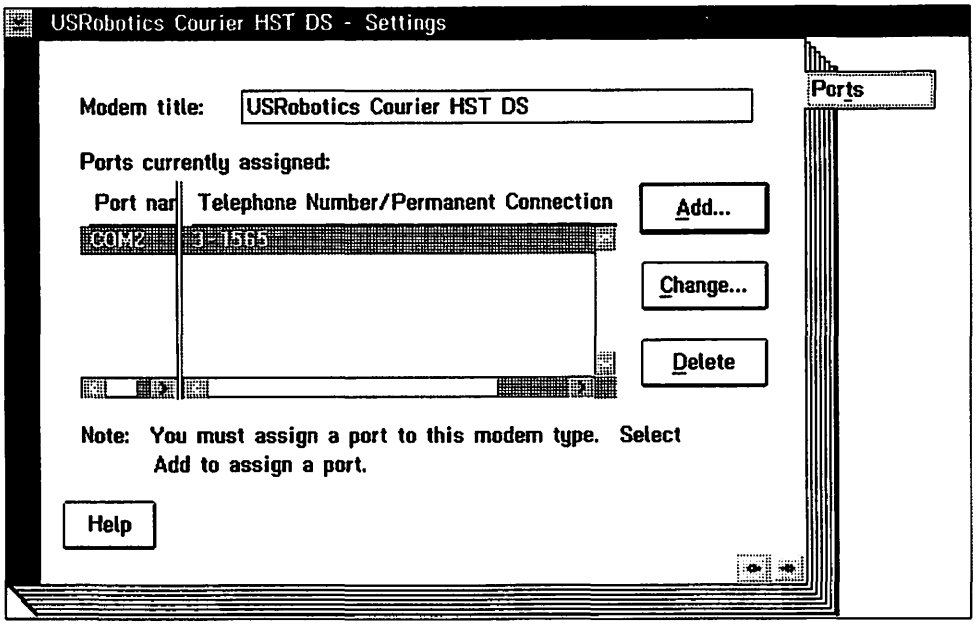


Figure 238. Ports Currently Assigned Window

10. If you are using the same modem type for another port, then select the **Add** button to add one more port to this modem type.
11. Close the window when no more ports should be added to this modem type.

    The Modem type assignments list at the Modems tab has now been updated, as shown here:

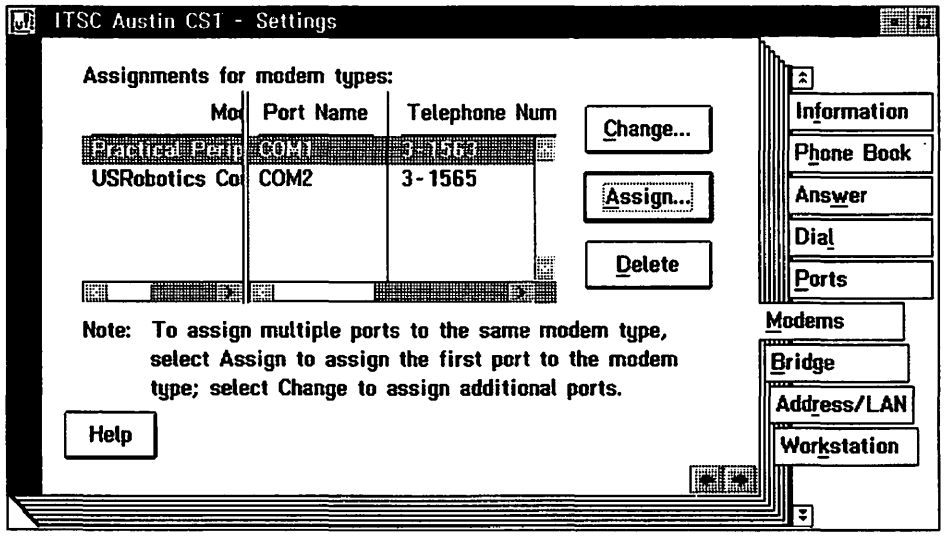


Figure 239. Settings Notebook, Modems Tab

12. If there are any more ports to add then:
    - Select the **Assign** button if it uses a new modem type.
    - Select the **Change** button to add more ports to an already used modem type.
13. The configuration is completed when all ports are added.
14. Close the Settings notebook to save the configuration.

15. Shut down and restart the Connection Server.

Configuration of the multiple lines is now completed and the new lines are ready to use.

After successful ports and modem configuration, you can view the ports in the Call and Port Management section of the Connection Server

7.11 Implementing Security

Adding remote access capabilities to your LAN can make your LAN and its resources vulnerable to unauthorized remote access. The security features provided by the Remote Access Services product control access to the Connection Server and help prevent LAN access by unauthorized users.

The Remote Access Services security subsystem provides two main services:

1. It protects the LAN from casual, unauthorized external access.

   When an external WAN circuit is established at a &CS, the security service ensures that, until the caller is authenticated:

   - No LAN frames are transferred onto the WAN circuit
   - No WAN frames are transferred onto the LAN wire

   In addition, if there are already several external users that have been authenticated and are currently accessing an application server on the LAN, the security subsystem ensures that a new caller does not see any of the traffic between the LAN and any of these other users until the new caller has been authenticated.

   A new caller can learn nothing about the names being used on the LAN until the caller is authenticated. Also, a new caller cannot introduce any data (for example, inject error frames) onto the LAN until the caller is authenticated at the Connection Server.

2. Continuous validation of remote requests.

   When a Connection Server receives a request for service, it can determine whether the:

   - Request was sent by an authorized user
   - Request received has not been modified in transmission
   - Current message is not a copy of a prior message

   Before a Remote Workstation sends requests to a secured Connection Server, the user at the Remote Workstation must first be authenticated by the Connection Server.

Security Features

The Remote Access Services security feature is a configuration option that can be enabled on a Remote Workstation workstation as well on the Connection Server. This function is not available on Windows workstations (however if it is enabled on the connection server, then both the OS/2 and the Windows requester must supply a user ID and password).

If security is disabled, any person can access the configuration interface at the connection server and enable its security option. However, once security is

enabled, only a user designated as a security administrator can log on to the secured workstation and disable the security subsystem. Understand that the user database used for the Remote Access Services does not interface to any other user database (such as User Profile Management used by the File and Print Services).

Enabling or disabling security at a Remote Workstation is a local operation only and cannot be performed remotely. That is, a security administrator must be physically located at the machine when operating the configuration user interface that toggles the state of the security subsystem.

Password Phrases

To minimize the possibility of offline dictionary attacks to discover user passwords, the security database supports *passphrases*. Up to 32 case sensitive characters can be used to build individual tokens that comprise a password phrase. The passphrase is one-way encrypted using a *hash* algorithm. The resulting *password key* is 8 bytes in length.

Note: A hash algorithm is a method of transforming a *source key* to an *object key*. It is computationally difficult to derive the source key from the object key. The probability of two different source keys resulting in the same object key is extremely low.

User Permission Types

The user accounts database on each Remote Workstation is maintained independently. The Connection Servers user database can be configured to operate independently or to use a shared database. This database contains information on each user such as the user ID, password key, and user type. The three user types are:

- User

  This is the lowest security classification. A user of this type can also view and change selected information (for example, user description and user passphrase) within the user's own account at a secured workstation.

- Administrator

  This user type has the same privileges as a user type and is able to perform the following tasks:

  - Creating and maintaining dialing and answering specifications
  - Managing connections
  - Managing ports
  - Resolving error situations

- Security administrator

  This user type has the same privileges as an administrator and in addition, is authorized to maintain the *security policy* (for example, maximum number of logon attempts permitted during a single call). A security administrator can view, add, and delete user accounts within the user account database. This user type can change any of the account information contained in other users' accounts.

Single Logon

A user is required to log on and be authenticated by each Connection Server before accessing the server's services. For example, a user that has been authenticated can:

- Use Dialer services
- Use Management services
- Access the target LAN wire

However, a user need only be involved in a single logon task (that is supplying a user ID and passphrase) provided the user has the same user ID and passphrase at each of the secured Connection Server workstations that the user subsequently attempts to access. The user ID and password key used during the first logon are saved (in memory only) by the workstation security component and used first for each of the following logon attempts at the other secured Connection Servers. The user is required to participate in a second logon only if the user ID or passphrase is different at the next secured Connection Server .

If a Connection Server has security enabled then Remote Workstation users (both OS/2 and Windows) are prompted for the user ID and passphrase after they dial and establish a link with the connection server. If an OS/2 Remote Workstation has security enabled, then the user at that workstation must also log on *locally* before accessing local services (such as Settings). In addition, users at Remote Workstations (both OS/2 and Windows) attempting to access an OS/2 Remote Workstation where security has been enabled must first log on to that Remote Workstation, just as they would to a secured connection server. This additional function is not available for Windows Remote Workstation users.

If security is enabled at an OS/2 Remote Workstation and if the user ID and the passphrase match between the OS/2 Remote Workstation and the connection server, then the user is prompted for only one logon (the first local logon); an implicit logon occurs after a connection is established. If the user ID and the passphrase do not match between the &wr. and the connection server, the user is prompted to log on again to the connection server after the link has been established.

After the remote logon and filtering has completed, it is the responsibility of the LAN-based applications, such as OS/2 LAN Server, to provide security for their own applications. Logons to these applications are separate from the remote logon.

User Authentication Protocol

The Remote Access Services security subsystem implements a two-party, two-way entity authentication protocol based upon an IBM patented protocol called 2PP. The Remote Access Services user authentication protocol is based on the use of *Message Authentication Codes* (MACs).

The Message Authentication Code Standard ANSI X9.9, defines a process for authentication of messages from originator to recipient. A Message Authentication Code is an 8-byte *cryptographic* checksum attached to the message. It is derived using a secret key and the content of the message. The Message Authentication Code scheme uses *Data Encryption Standard* (DES) and adheres to the X9.9 standard.

After a successful mutual authentication (client to server and server to client) the client and server both share a session key that is used to build the certificates that authenticate all subsequent workstation service requests sent to the connection server. A different session key is used during each separate logon session. The protocol satisfies the following requirements:

- The protocol provides mutual authentication between a client and a server. In the process of authenticating one another, the client and server come to share a random session key.
- The client initiates the protocol. The client has no information about the server except the server's address. The client has a user ID and a user supplied passphrase for authentication.
- The server has no information about the client besides the client's user ID and passphrase derived key.

User Authentication Protocol's Data Flow

The protocol requires three rounds and is shown in the following picture.

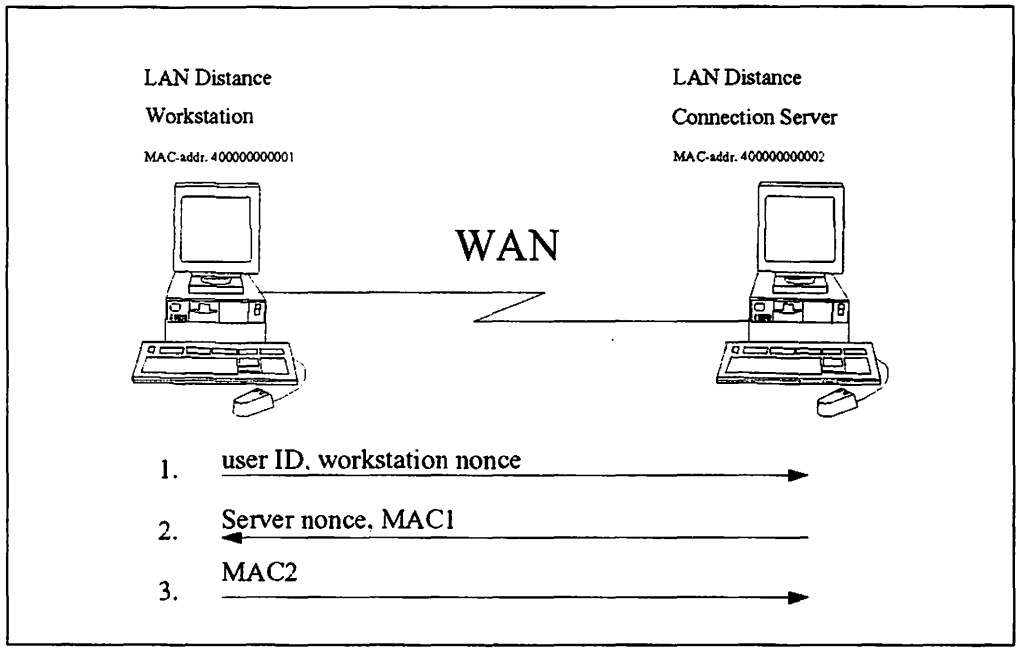


Figure 240. LAN Distance Protocol Data Flow. Although the user types in a user ID and passphrase, note that the passphrase does not go across the link.

Figure 240 shows you the protocol data flow.

1. In this protocol, a user on the Remote Workstation logs on to the connection server. The user submits only the user ID and the passphrase. The Remote Workstation actually sends the following to the connection server:
   - User ID
   - Remote workstation *nonce*. A nonce is a random value generated for this session only and will not be repeated in subsequent sessions.

   Note: The user passphrase, its associated one-way encrypted password key, and the resulting common session key do *not* appear on the link. A new one-way encrypted password key derived from a new passphrase (that is, when the user changes the passphrase) does appear on the link, but it is encrypted using the logon session key.

2. The connection server responds by creating its own server nonce and returns both the connection server nonce and a Message Authentication Code (MAC1) based on the following information and encrypted using the one-way encrypted password key from the user's database account:
   - User ID
   - Remote workstation nonce
   - Connection server nonce
   - Connection server LAN adapter address (400000000002)

   Since the Remote Workstation also knows the above information, the Remote Workstation can generate the same MAC1 using the one-way encrypted password key derived from the passphrase supplied by the user.

   The Remote Workstation compares the Message Authentication Code (MAC1) received from the connection server with its locally generated Message Authentication Code. If they match, the Remote Workstation accepts the connection server as authentic.
3. The Remote Workstation then returns a new message authentication code (MAC2) back to the connection server based on:
   - Workstation nonce
   - Connection server nonce

   When the connection server receives MAC2, it computes its own Message Authentication Code based on the same information, and compares its code with the one received from the Remote Workstation.

   If the two codes match, the connection server accepts the Remote Workstation as authentic.

As a result of the exchange, after each side has authenticated the other side, each party separately generates a common *session key*. It is good for that session only.

Note: The session key never goes across the link.

This session key is then used to verify all Remote Access Services commands. The session key is not used to verify data for other applications going across the link.

If the Remote Workstation user is authenticated successfully (that is the user provides the correct passphrase), the Remote Workstation can generate *server certificates* (that is, Message Authentication Codes) that can be added to requests sent to the connection server.

When a connection server receives a request containing a certificate, it can validate the certificate and verify that the user sending the request is authentic and authorized by the connection server to request the service.

Moreover, a valid certificate contains proof that the request itself has not been modified since being sent and is not a copy of a certified request (sent earlier by a valid user) that was introduced by a hacker masquerading as the valid user.

The protocol of Figure 198 on page 282 may be subject to dictionary attacks if the user fails to take advantage of the capability of a full passphrase (for

example, a single word is used for the passphrase instead of a passphrase such as, *These are my hot new BOOTS*).

Security Policy Options

Several user authentication *security policy* options can be configured by a security administrator when setting up a connection server, such as the following:

Note: Security policy is a set of rules that can be customized to enable the security requirements of a particular user environment.

- Maximum Age

  Users with passphrases are required to change their passphrase when the age of their current passphrase exceeds this time period.

  The user is not permitted to log on until a valid new passphrase has been submitted. The new passphrase does not take effect until the next logon (that is the current passphrase is used for the passphrase change session). The user is permitted to change their own passphrase prior to the passphrase's expiration time using a separate user account management interface. The default is 30 days and a no maximum selection is supported.

- Minimum Age

  A security administrator can specify a time period during which a user is unable to change a recently established passphrase.

  The default time period is 0 days, which means that there is no restriction on when a user can change a newly assigned passphrase.

- Minimum Length

  A security administrator can establish the minimum passphrase length that is required for each user account. The minimum passphrase length can be from 4 to 32 characters.

  The default is 8 characters.

- Duplicates Checked

  A security administrator can specify that a history of from 0 to 8 prior passphrases be saved in the user's account. Whenever the user changes his/her passphrase, the new passphrase is checked against these passphrase history values to ensure the new passphrase is not a duplicate of a recent passphrase. If a duplicate is found, the new passphrase submitted is reported to be invalid and the user is asked to submit another new passphrase.

  The default is 8 prior passphrases.

- Maximum Logon

  A security administrator is able to specify the number of unsuccessful logon attempts that are permitted. A logon attempt can fail because:

  - Unknown user ID is submitted
  - Inactive account is being accessed
  - Passphrase is incorrect
  - User is calling from a workstation with a LAN adapter address that is invalid for the account

- User is calling during a day of the week or a time of the day that is invalid for the account

The maximum number of allowed logon attempts defaults to 4.

If the maximum number of logon attempts is exceeded, the user's account is automatically marked as inactive. In this situation, in order to log on in the future, a user is required to contact the security administrator to have the account reactivated.

Additional Security Options

This section covers additional security options that are available. These are:

- Callback
- Workstation Address
- Logon Time intervals

Callback

The Remote Access Services security supports an optional *Callback* feature for Remote Workstations only. Callback to Remote Access Services requesters and a connection servers are not supported. The Callback option configured within the caller's account is not checked unless the call is placed from a Remote Workstation.

Note: Callback is a feature, active during LAN Distance connection establishment, in which the answering workstation re-initiates the connection by placing a Callback to the dialing workstation. The original dialing workstation must be a Remote Workstation.

Figure 241 on page 338 shows you the general Callback procedure.

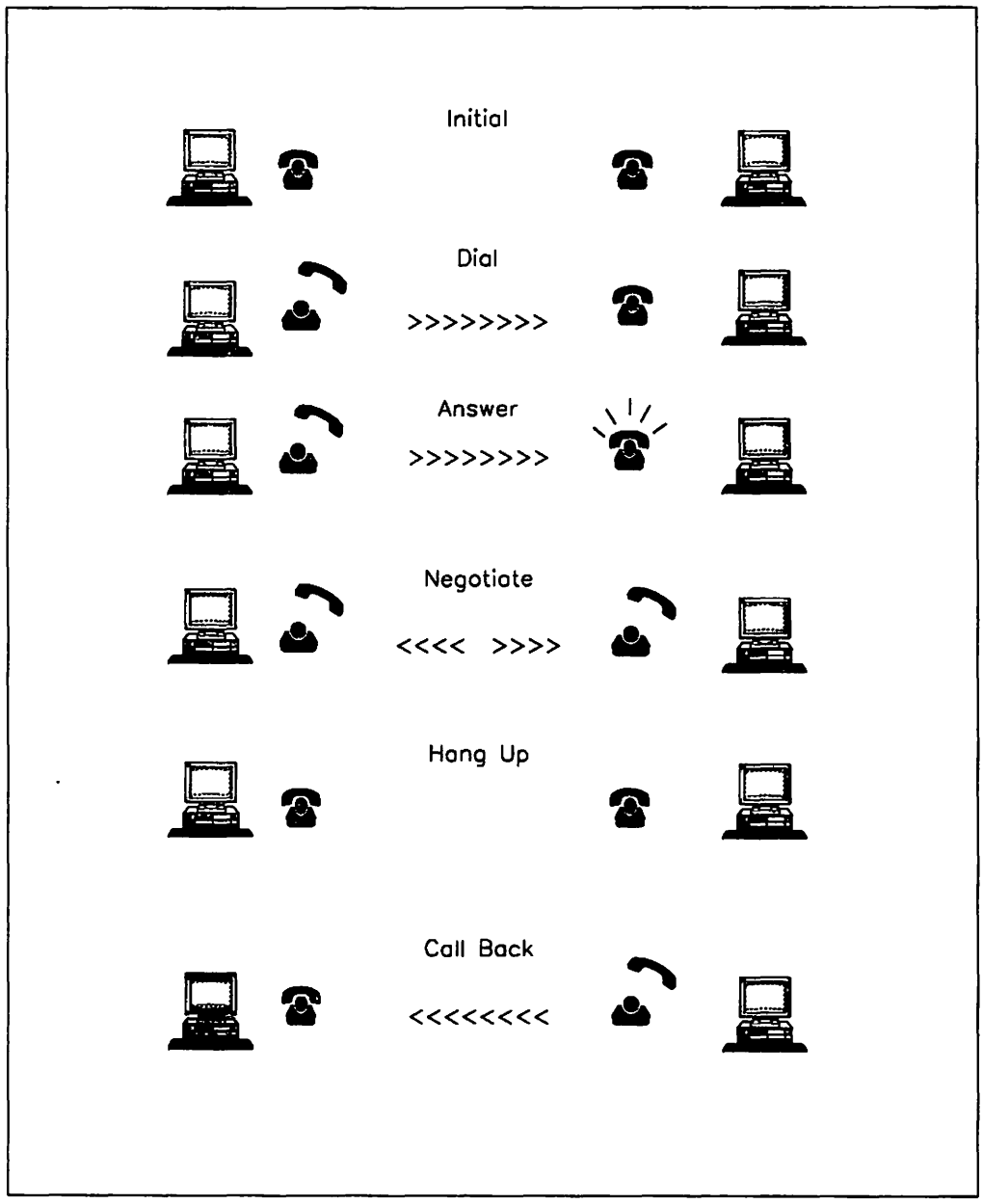


Figure 241. Callback

Callback can be configured in a user account as follows:

- Calllback not required

  These users are never called back by the called connection server.

- Fixed callback

  These users are called back at a fixed configured telephone number.

- Mobile callback

  This is part of the logon protocol. The connection server can then use the telephone number submitted to it for the callback.

The caller is authenticated both:

- Prior to the callback (this prevents harassment calls)

- After the callback is complete (this guards against known hacker techniques that can normally only be avoided using special telephone equipment or service options)

Callback can be useful if reversal of telephone charges is needed. For example the majority of the charges for a call from a hotel room can be charged to the central site instead of the traveler at the hotel.

Workstation Address Identification

A security administrator can configure up to eight workstation LAN addresses within a user account. The caller must call from a workstation that has been configured with a Remote Access Services logical adapter network address that matches one of the MAC addresses stored in the caller's account; otherwise, the logon attempt fails.

Valid Logon Time Intervals

A security administrator can configure the days of the week and the time of the day during these weekdays that a user is allowed to log on to his account at the connection server.

A logon attempt at a time that is not within the specified time intervals specified in the user's account, fails.

Protecting your Passphrase

The following diagram shows you what to consider if you work with Remote Access Services and need to log on to different systems in the LAN (for example to the OS/2 LAN Server and to a 3270 host).

Important

It is assumed that connection servers are physically secured. Access should be limited to a few trusted administrators.

In Figure 242 on page 340, you can see that a user on a Remote Workstation that would work with the OS/2 LAN Server and a S/370 host has to make a logon (with a user ID and a password) to:

1. Remote Access Services
2. OS/2 LAN Server
3. S/370 host

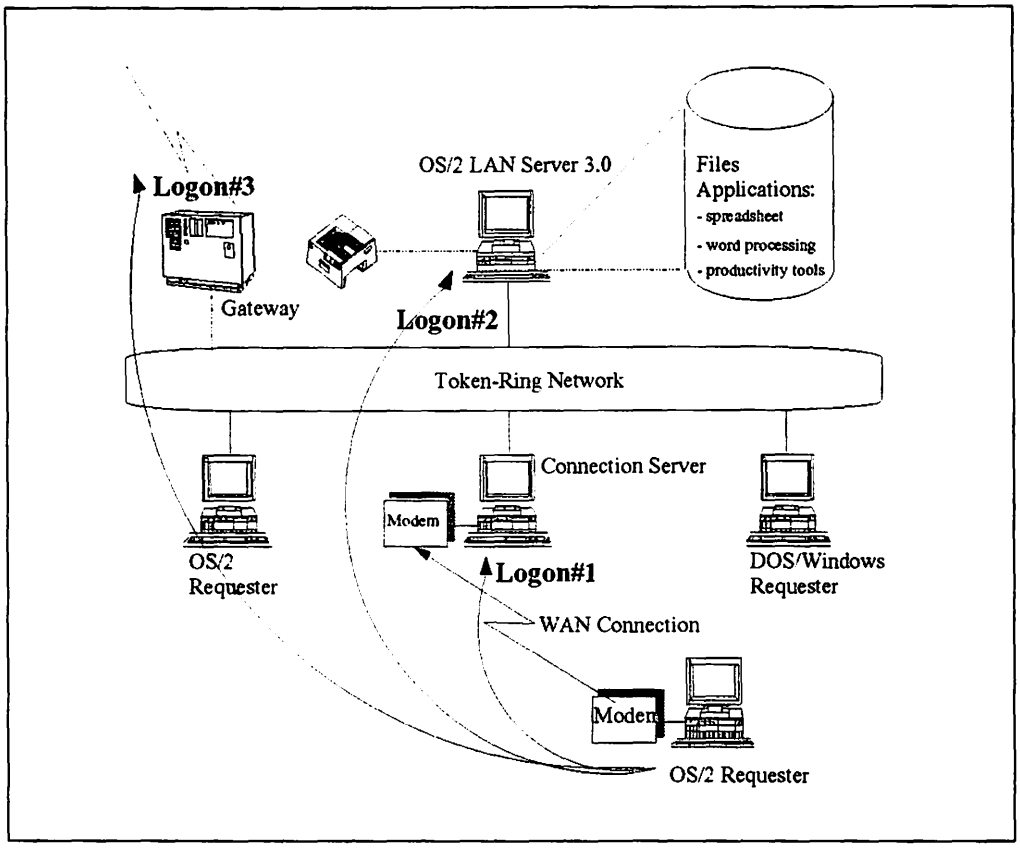


Figure 242. Protecting Your Passphrase

Note: Make certain the passphrase used to log on to the connection server and the passwords used for the OS/2 LAN Server and 3270 host sessions are different. This is important because *Remote Access Services does not encrypt application data that appears on its link*. Special equipment (such as a LAN sniffer) cannot see the Remote Access Services passphrase, but can see other passwords from other applications that do not encrypt their passwords. So, use different passwords for &ld. and for other applications and inform the Remote Workstation users about this rule.

If you have used the same password for Remote Access Services and your 3270 logon, a hacker may trace the communications link, identify the 3270 password, and try this password for the Remote Access Services passphrase. This may enable a hacker to dial into your LAN.

Enabling the Remote Access Services Security Options

The Remote Access Services supports two optional types of security for restricted access to the LAN and its resources. The first type of security is included with the Remote Access Services component and is provided by the User Account Management. The second type of security that Remote Access Services supports is a User provided *User Exit Package*. Remote Access Services supports any OEM-provided security user exit package that is developed in conformance with the LAN Distance Generalized Security User Exit API.

You can also set up the Remote Access Services to use either or both of the security options defined above. By default security is disabled. The Remote Access Services Notebook is used to enable security. Before security can be

used it must be enabled. To enable Remote Access Services security complete the following steps:

- From the Settings notebook, select the **Security** tab. The following window is displayed.

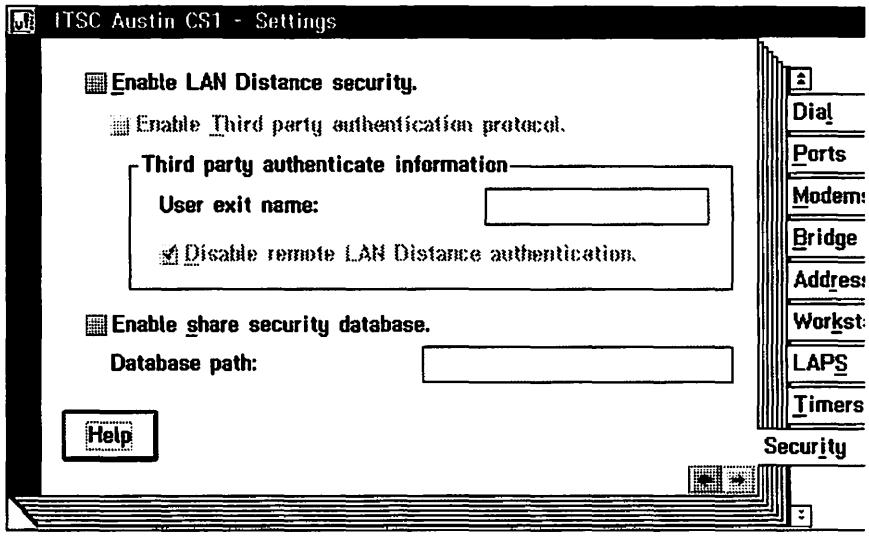


Figure 243. Settings Notebook, Security Tab

- To enable security you have the following options:
  - **To Use of only LAN Distance Security**

    Select just the *Enable LAN Distance security*
  - **To Use LAN Distance Security and a Third Party authentication protocol**

    To make use of both security options select the *Enable LAN Distance security* and *Enable Third Party authentication protocol.*

    When Enable Third party authentication protocol is selected, you must provide a User exit name. This name can be up to 8 characters. *Do not* specify the DLL extension.
  - **To use just a Third Party authentication protocol**

    To make use of just the Third Party authentication you need to select the *Enable LAN Distance security* and the *Enable Third Party authentication protocol.*. After supplying the user exit name you need to select the *Disable remote LAN Distance authentication*
- To enable the sharing of the security database select **Enable share security database**. This applies if you have multiple Remote Access Services and wish to share a common security database. The Location field is the drive and path to the shared security database. You can specify a maximum of 127 characters. This field is optional.
- After specifying the security options close the settings notebook and the Remote Access Services application. Once the Remote Access Services application restarts security will be enabled.

User Account Management

If you have selected to use the security provided with the Remote Access Services, you will need to define the users. After resetting the Remote Access Services server, you will now need to log on to your secure Remote Access Services

Now you have successfully enabled the security option. The following sections show you how to customize the different security options. These tasks are presented in more detail in the following sections:

- Logging on for the first time
- Setting up Personal Account Information
- Adding a new user:
  - Specifying the user type
  - Specifying the user's passphrase
  - Specifying the user's logon interval
  - Specifying the user's addresses
  - Specifying the user's callback feature
- Defining the policy options

Logging On for the First Time

After restarting the Remote Access Services program, you have to perform a first logon as a security administrator to configure all the security options.

1. Select **Selected** from the menu bar.
2. Select **Logon**.

   The LAN Distance Logon window is displayed as follows:

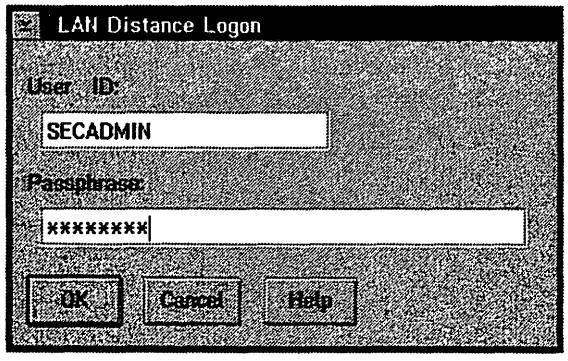


Figure 244. LAN Distance Logon

   In Figure 244 you have to enter the default user ID and the default passphrase.

3. Enter the default *user ID*, that is: **SECADMIN**.
4. Enter the default *Passphrase*, that is: **SECADMIN**.

   Note that the passphrase is case sensitive. You have to enter the passphrase *SECADMIN* in uppercase letters.

5. Select the **OK** button.

   The following message window is displayed:

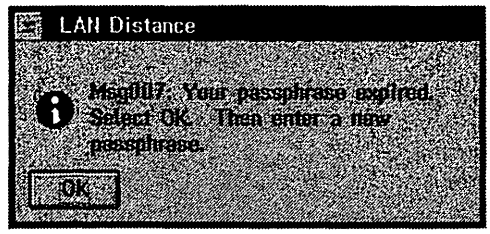


Figure 245. Passphrase Expired

This message tells you that the passphrase is expired and forces you to enter a new passphrase to replace the default passphrase.

6. Select the **OK** button.

   The following Change Passphrase window is presented:

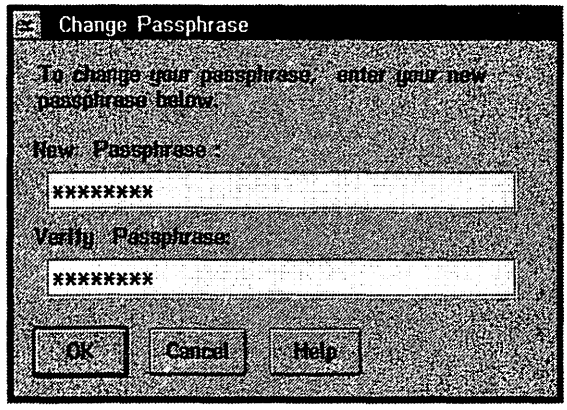


Figure 246. Change Passphrase

7. In the **Change Passphrase** window, enter: A new passphrase in the *Change Passphrase* and re-enter the passphrase in the *Verify Passphrase* field.
8. Select the **OK** button.

If you enter a valid new passphrase, you are logged on as a security administrator. You are now able to configure all the security options.

Note: The new passphrase length must be greater than the default policy for minimum password length, which is 8 characters.

Setting Up Personal Account Information: This section shows you what you can see and what you can change in the Personal Account Information section.

Perform the following steps as shown in Figure 202 on page 290 :

1. Select **Selected** from the menu bar.
2. Select **Open as →**.
3. Select **Personal Account Information**.

You now see the Personal Account Information window (General section) as shown in Figure 247 on page 344.

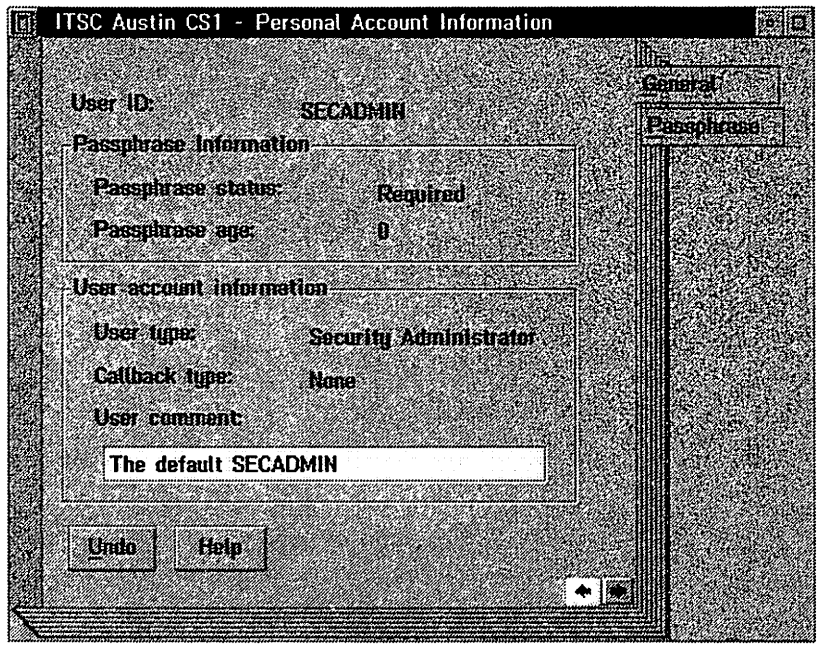


Figure 247. Personal Account Information (General Section)

The following two information sections are presented:

- **Passphrase Information**

  This section gives you information about the passphrase status and the passphrase age.

  - **Passphrase status**

    This field specifies whether a passphrase is required for logon.

  - **Passphrase age**

    This field specifies the age of your passphrase in terms of number of days.

- **User account information**

  This section gives you information about your user type, type of callback and a description of your user account.

  - **User type**

    This field displays the privilege level of your user account (that is, user, administrator or security administrator).

  - **CallBack type**

    This field displays the type of callback to be performed for your user account.

    - **Fixed Callback** restricts your dialing location to a fixed location that does not change.
    - **Variable Callback** allows your dialing location to change. For example, if you are traveling, you can dial in from a customer location or a hotel.

Select the **Passphrase** tab from the Personal Account Information notebook and the following window is displayed:

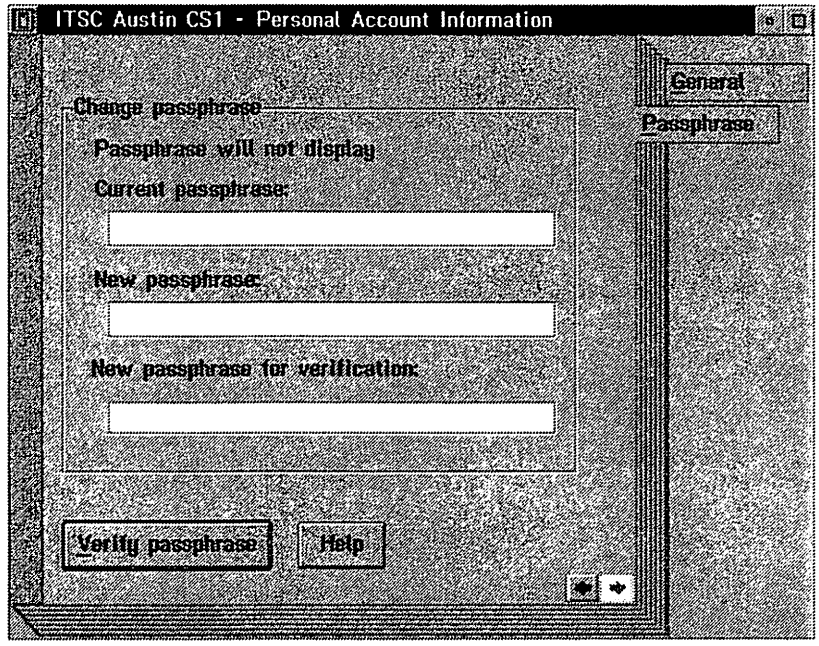


Figure 248. Personal Account Information (Passphrase Section)

Note: In this section, you can change the passphrase for your personal user account.

Adding a New User

This section describes how to add a new user. First, you need to:

1. Select **Selected** from the menu bar.
2. Select **Open as →**.
3. Select **User Account Management**.

The User Account Management window Account section, as shown in Figure 249 on page 346, is presented.

A user account must exist for every user that is authorized to remotely access this secure LAN Distance workstation.

A security administrator can manage the user accounts of all other users with the User Account Management functions. Each user and administrator is limited to changing only the passphrase and description for their own personal user account.

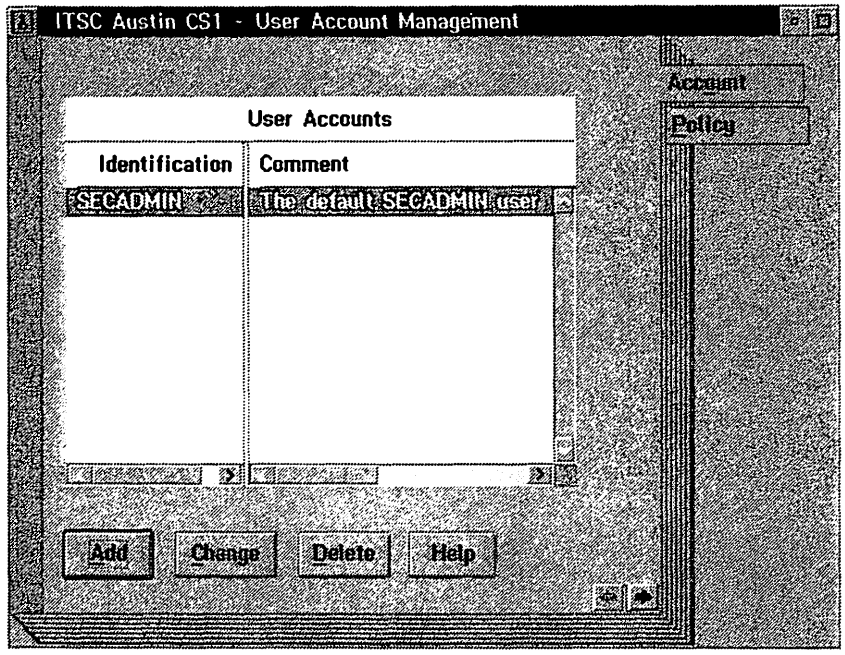


Figure 249. User Account Management Window (Account Section)

The following steps show you how to set up a new user account:

1. In Figure 249, select the **Add** button.

   The Type tab of the user account notebook that is now presented displays information about the user account, including:

   - User ID
   - Comment
   - User type (user, administrator, or security administrator)
   - Account Status (inactive or active)

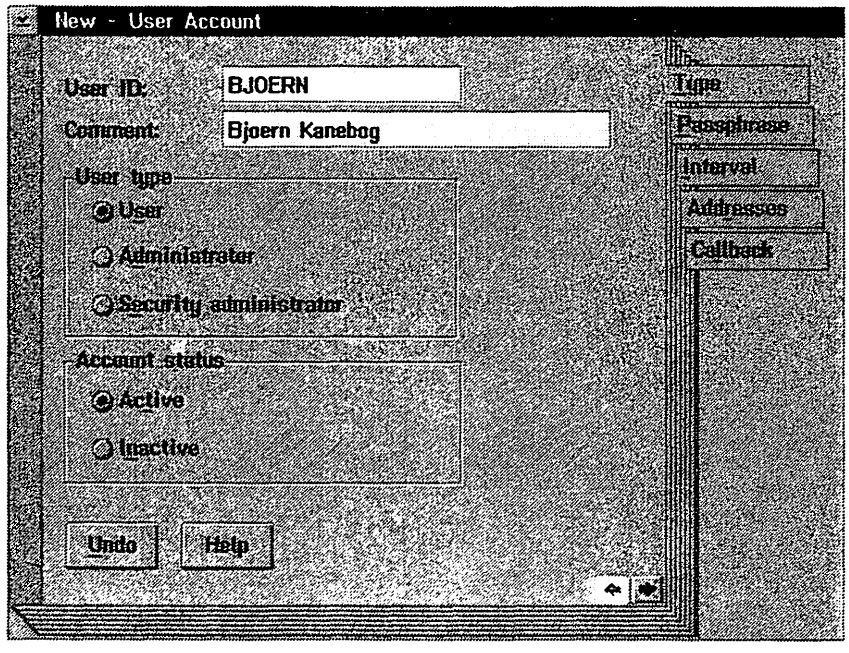


Figure 250. New - User Account Window (Type Section)

2. In the User ID field, enter the new user ID.
3. In the Comment field, enter the user's name.
4. In the User type section, select **User**.
5. In the Account status section, select **Active**.

   Note: The Account status indicates whether or not security can access this user account for user authentication.

   A user account can be either Active or Inactive. Making a user account Inactive is a method of denying remote access by a particular user, without deleting the information in that user account.

   A user account can be deactivated, meaning that it cannot be accessed by the user authentication functions. By deactivating a user account on a secure Remote Workstation, you restrict that user from accessing the workstation. The benefit of deactivating a user account, versus deleting it, is that the information in the user account is preserved.

   Note: A user account is automatically deactivated when a user exceeds the limit for unsuccessful logon attempts.

   To deactivate a user account, change the Account status field to Inactive.
6. Select the **Passphrase** tab from the New - User Account notebook.

   The Passphrase tab of the User Account notebook that is now presented is used to manage the passphrases for this user account, including:

   - Specifying if a passphrase is required to log onto this secure Connection Server
   - Specifying a passphrase if adding a user account
   - Changing a passphrase if changing a user account

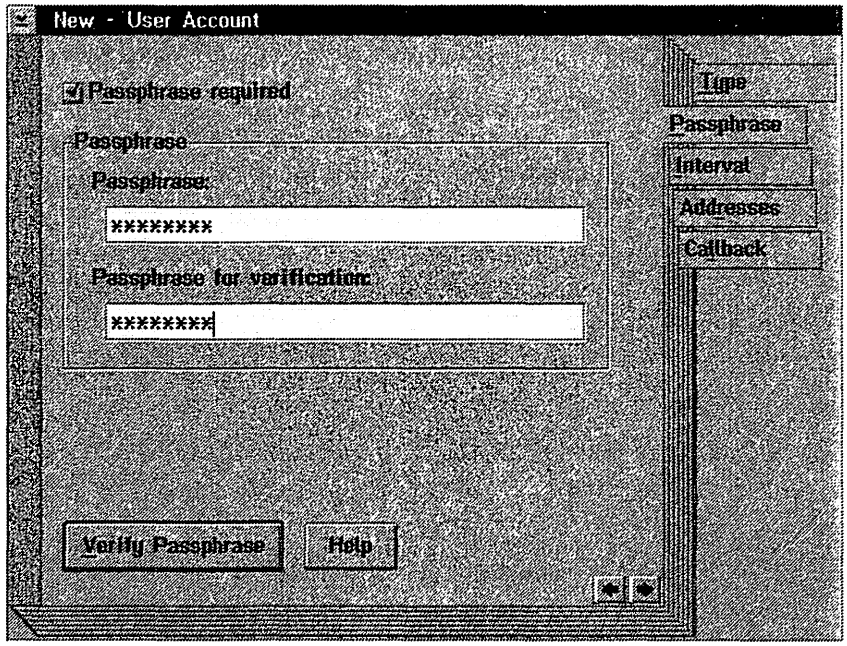


Figure 251. New - User Account Window (Passphrase Section)

7. Select the **Passphrase required** checkbox.
8. In the Passphrase field, enter a passphrase.

9. In the Passphrase for verification field, enter the same passphrase for verification.
10. Select the **Verify Passphrase** button.
11. Select the **Interval** tab from the New - User Account notebook.

    The Interval tab of the User Account notebook that is now presented is used to manage the logon time intervals for this user account.

    Note: Multiple logon time intervals can be specified for a user account. If logon time intervals overlap, the earliest time is used as the starting point and the latest time is used as the stopping point.

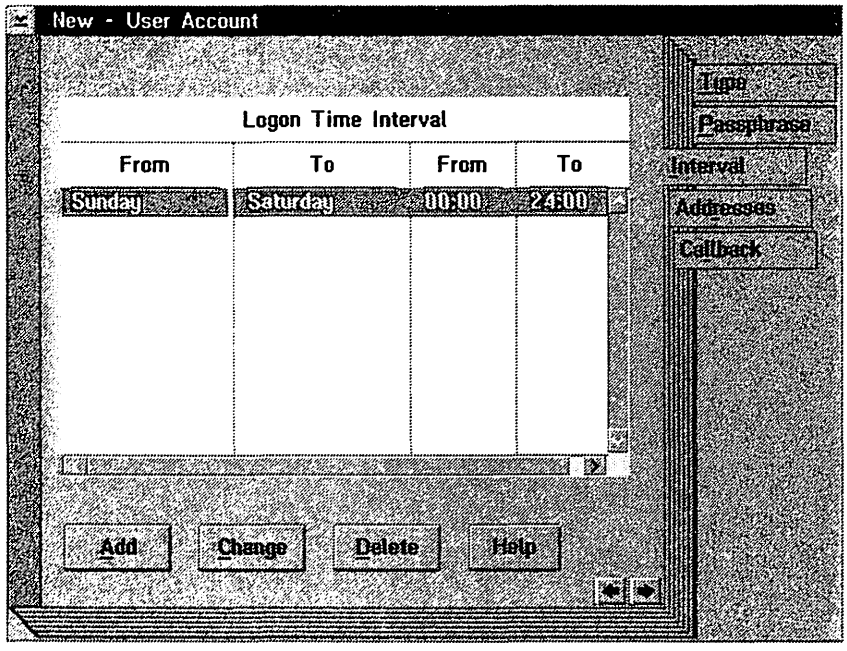


Figure 252. New - User Account Window (Interval Section)

Figure 252 shows you that the default logon time interval is from Sunday to Saturday and from 00:00 to 24:00. That means that the default has no limitations. A user with the default can log on at any time.

In our example, we define limitations because, in our company, we would like to save energy on the weekends, and during 22:00 and 05:00, we run some special procedures, such as a backup programs.

12. Select the **Change** button.

    The following window is presented.

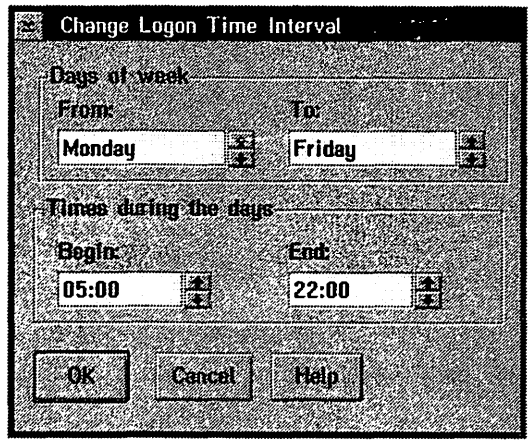


Figure 253. Change Logon Time Interval Window

Figure 253 shows you that in the Days of week section, we selected:

- From Monday to Friday.

In the Times during the days section we selected:

- Begin: 05:00 and End: 22:00

13. Enter your own values.
14. Select the **OK** button.

    The result of this change is shown in Figure 254.

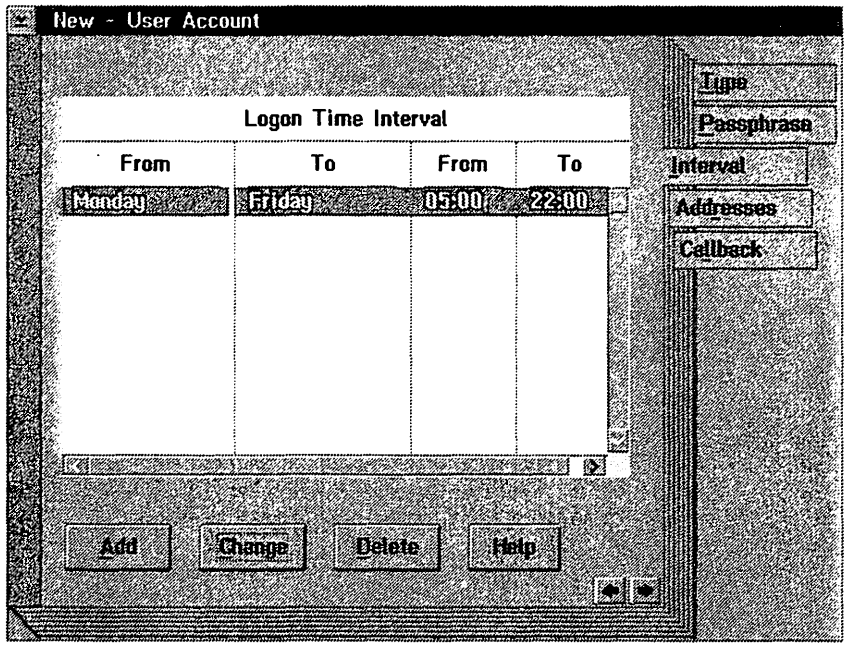


Figure 254. New - User Account Window (Interval Section)

15. Select the **Addresses** tab from the New - User Account notebook.

    The Addresses tab of the User Account notebook that is now presented is used to manage the LAN Distance logical adapter network addresses.

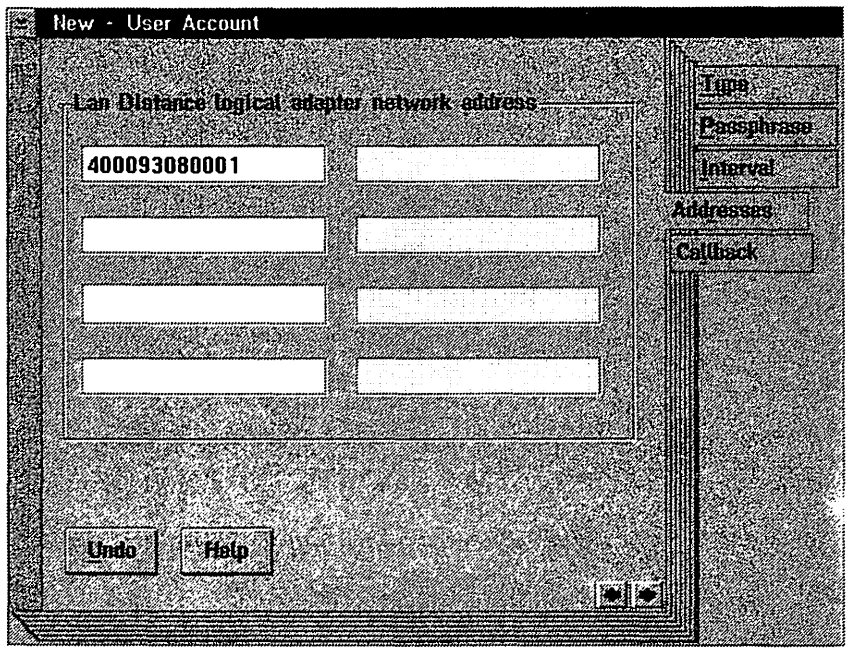


Figure 255. New - User Account Window (Addresses Section)

Figure 255 displays the logical adapter network addresses of the valid workstations for this user account. Use this tab to view or update these logical adapter network addresses.

If no logical adapter network addresses are displayed, the user can access the Remote Access Services from any address.

We specified the adapter number **400093080001**. That means the user can only log on from a workstation with that adapter number. If the user needs to be able to log on from different workstations, you can specify up to eight adapter numbers.

Note: The user must use one of the specified workstations to access this Remote Access Services. When the user attempts to log on to this workstation, his actual logical adapter network address is verified against this list.

16. Specify your adapter numbers here if your user should be able to log on from one or up to eight different workstations.
17. Select the **Callback** tab from the New - User Account notebook.

    The Callback tab of the User Account notebook that is now presented is used to manage callback options for this user ID.

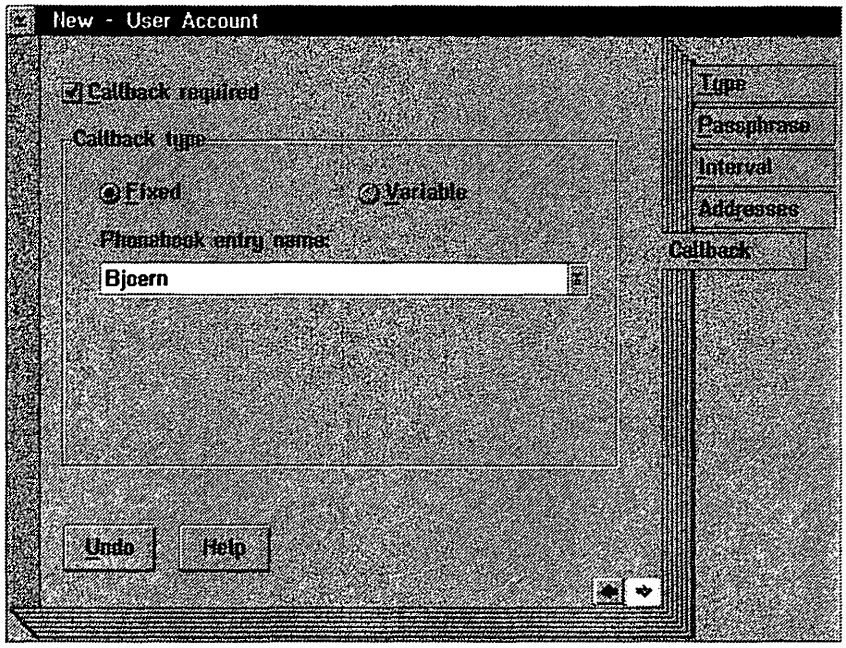


Figure 256. New - User Account Window (Callback Section)

Figure 256 shows you the group of fields which display the type of Callback that is performed for this user account.

18. Set the Callback required field to **On.**
19. Set the callback type to **Fixed**.

    Fixed or Variable is used to specify the type of callback for this user account. Callback can be performed to either a fixed or variable location. If the dialing user's location does not change, then Fixed Callback should be selected. If the dialing user's location is subject to change, as is the case for a traveling employee dialing in from a customer location or a hotel, then Variable Callback should be selected.

    Note: Fixed and Variable are available only if Callback required is selected.

20. Type in a Phonebook entry name in the Callback type section.

    Note: If Callback is required, you must specify the Phonebook entry name that corresponds to the dialing user's location.

    Phonebook entry name contains connectivity information that is needed in addition to a phone number. A Phonebook entry name for Fixed Callback must have a phone number, but a Phonebook entry name for Variable Callback does not require a phone number.

21. Close the New - User Account window.

Defining the Policy Options

1. Select the **Policy** tab from the User Account Management notebook.

   In Figure 212 on page 300, the values shown in the window are the defaults.

   For more information about these options, refer to section "Security Policy Options" on page 336.

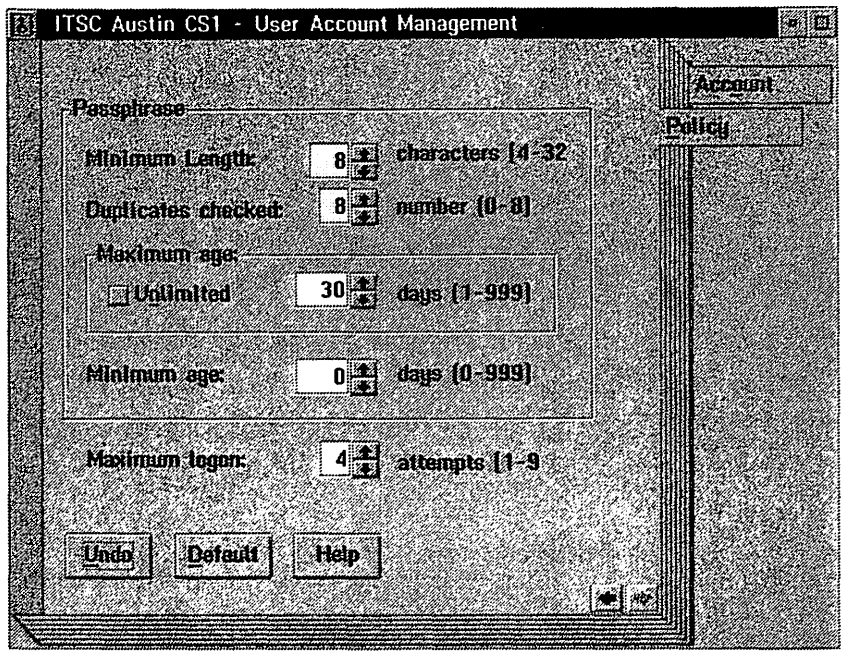


Figure 257. User Account Management Window (Policy Section)

Attention

Please ensure that you define in the Passphrase section the Minimum Length field greater than 8. That means set that value, for example, to 20 or even better, 30. This forces the user to enter a passphrase different from the password of the OS/2 LAN Server or the password he has to enter to log on to a 3270 host. See section "Protecting your Passphrase" on page 339 for more details.

2. Enter your own values.
3. Close the User Account Management window.
4. Close the Connection Server program.
5. Restart the Connection Server.

Security User Exit Package

The security user exit package consists of two user-exit modules: one for the client and one for the server. The client and server user-exit modules work together to implement the user authentication protocol defined by the security user-exit package.

A user authentication protocol is a series of user-exit messages/tokens exchanged between the client and server user exit modules when validating the user of a Remote Workstation that is calling a Connection Server

One client workstation can use a different security user exit package to access each different Connection Server it calls. A Connection Server can use only one security user-exit package to allow access from all remote workstations that call it.

Security user-exit packages can be used with or without Remote Access Services security (User Account Management). If LAN Distance security is used

with the security user-exit package, the authentication will take place first through the user-exit and second through LAN Distance security.

A development toolkit for the LAN Distance Security User Exit for OS/2 and Windows is available. The toolkit contains:

- Specification of the LAN Distance Generalized Security User Exit API
- Description of how a LAN Distance security user exit can be installed/registered at LAN Distance workstations
- Sample source code for developing your own LAN Distance security user-exit package

The toolkit is available through IBM Service and Support by referencing APAR IC07742.

Shared User Database

A large environment that has the requirement for multiple Remote Access Services servers poses some problems. One of them being that of registering users on each server. With previous versions of LAN Distance Connection Server the user database had to be duplicated. Previous versions of LAN Distance also allowed only one Security administrator to log on at any one time. One of the new features of Remote Access Services is the ability to share the user database between servers and allow multiple administrators to log on simultaneously.

The database sharing is achieved by using a shared file on a redirected drive provided by a File Server. In this way multiple Remote Access Services servers can share the Security Database file. The integrity of the Security Database is protected by serializing all modify request to the Security Database.

Because the Remote Access Services servers rely on the File Server to access the database, this file service should be up and running at all times. One of the problems that one may encounter while running in SHARE mode is that of Database backup. The Remote Access Services does not provide a Database backup mechanism, it relies on Network software for the backup.

If you have multiple Remote Access Services in your network you will need to do the following to enable the sharing of the user Database. In this scenario we have two machines a Remote Access Services machine and a LAN Server machine. The Remote Access Services machine has LAN Requester loaded.

1. At the machine, on which you installed File and Print Sharing Services, create a new user ID that all Remote Access Services server will use, that will share a common Remote Access Services user database. For example: RASUSER.
2. Create and configure the shared directory.
   a. At the machine, on which you installed File and Print Sharing Services, create a directory alias named for example RASDB in the following fashion (assuming you want to put the shared database onto the server's D: drive):

```
Alias        RASDB
Description  RAS Security Database
Server name  <your server name>
Path         D:\RASDB
```

b. Select the radio button for sharing the directory alias at server startup.

c. Select the radio button for unlimited concurrent connections.

d. From an OS/2 command prompt, create a WAL directory below D:\RASDB.

e. When prompted create an access control profile permit the user named RASUSER (you created in the step before) read, write, and execute access rights to the RASDB directory alias.

f. Copy a new WCBUSRF.ISF from the OS/2 Warp Server WAL directory to the WAL directory that the RASDB alias points to.

3. Have OS/2 LAN Requester set up at the Remote Access Services machine.

   a. Ensure that the LAN Requester is working.

   b. Edit STARTUP.CMD and make following appends to it:

   ```
   LOGON RASUSER [/P:password]
   NET USE X: RASDB
   ```

   Note: Alternatively you could have given the user RASUSER logon assignments so that a `NET USE` command would not have been necessary.

4. Start the Remote Access Services service and modify the settings.

   a. Configure the Security tab.

   b. Choose enable Security.

   c. Choose shared....

   d. Type the path to the share database for example: X:\WAL.

   e. To set up additional Remote Access Services servers repeat step three for each additional machine. You will not need to create a user ID for each Remote Access Services server unless you changed the default setting for multiple logons to no at the File and Print Sharing Services server.

Security Database Tools

To manage the user information contained within the Security Database a few command line tools have been made available. These tools allow you to backup, add and print user information from the command line.

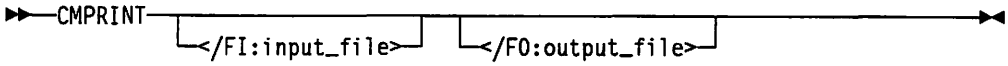
Backing Up the Database

The backup command is used to make a backup of the Remote Access Services Security Database. The command can be run while the Remote Access Services is up and running.

where `output file` is the name of the backup file the user wants to save the security database to. If this option is ignored the default backup file is WCBUSRF.BAK.

Print the Database

This function allows you to print all of the user IDs and user comments in the Remote Access Services security database into a specified file.

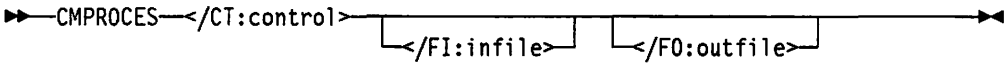


All of the parameters to this command are optional. The </FI:input_file> parameter specifies the name of the input Remote Access Services Security Database file. The default is WCBUSRF.ISF. The </FO:output_file> parameter specifies the name of the output file. The default is CMPRINT.REP.

Adding a User

This tool provides a batch processing capability for the Remote Access Services to add user data to the Security Database. This tool reads user information from a script file and adds the user data to the security database.

The tool requires the Remote Access Services to be up and the Security Administrator to be logged on before it can perform the task.



The control parameter /CT:control has two options: AD for add user to database and ME for merge the database.

The output file name parameter /FO:outfile is the name of the report file. This report file contains the user IDs and the return code of the requested action. The default output file for ADD user is CMADD.REP.

/FI:input is the input file name parameter. If the control parameter is AD the input file is a script file containing user information to be added. If the control parameter is ME the input file is the security database to be merge. The default filename of the input file is WCBUSRF.ISF

The format of a script file for adding users is one line of user information per user. The user information line contains the control key and user information as shown in the following format:

/ID:user ID /PW:passphrass /CM:user_comment /UT:user_type

Where:

/ID: specifies the maximum length of the user ID (must not exceed ten characters). This control key is required. The user ID is case insensitive.

/PW: specifies the maximum length of the passphrase (must not exceed 32 characters). If this control key is ignored then the passphrase of user account is set to not required. The passphrase is case sensitive.

/CM: specifies user comment. It is optional. The maximum length of user comment is 40 characters and case insensitive.

/UT: specifies the user type. It is optional and the default is USER.

There are three types of users available:

- U for type USER

- A for type ADMINISTRATOR
- S for type SECURITY ADMINISTRATOR

7.12 Application Considerations

This section will describe certain considerations when using particular LAN applications. This section will not cover all applications. For further information refer to the documentation referenced at the end of this chapter.

It is always best to install all the applications before installing the Remote Access Services client. Test the application locally to check that it works before attempting to run it remotely. This will enable you to narrow the problem down.

LAN Server and LAN Requester

Because of the slower data speeds over the Remote Access Services connection, you may experience problems with large file transfers, the XCOPY command, session timeouts and logging on to a server.

In order to avoid these problems you need to make some changes to LAN Server machines and LAN Requesters. Specific information about these parameters can be found in the respective INI files and the product documentation.

NetBIOS Timers

The NetBIOS Timers are automatically adjusted when Remote Access Services is installed on any connection server or remote workstation. You will need to set the NetBIOS timers of LAN Server machines that remote machines need to access. The NetBIOS timers can be changed by configuring MPTS or editing the PROTOCOL.INI.

Table 67 shows the guidelines for changing NetBIOS timers. For the LAN Server, or other machines that need to communicate with remote machines you will need to change these timers.

When changing the NetBIOS timers you should always maintain the following relationship.

```
Acknowledgment timer <= Response timer <= Inactivty timer
```

Table 67 (Page 1 of 2). Guidelines for Changing NetBIOS Timers

NETBIOS TIMERS	DESCRIPTION OF NETBIOS TIMERS
INACTIVITY TIMER- TI	The value for this timer determines how often NetBIOS checks an inactive link to verify that the link is still operational The NetBIOS default value for this timer is 30,000 milliseconds, increase the setting for this timer to 60000.
RESPONSE TIMER -T1	The value for this timer specifies the delay that should occur before retransmitting an unacknowledged frame The NetBIOS default value for this timer is 500 milliseconds. Increase the setting for this timer to 10000. As a rule, the response timer (T1) should be 2-5 times larger than the acknowledgement timer (T2).

Table 67 (Page 2 of 2). Guidelines for Changing NetBIOS Timers	
NETBIOS TIMERS	**DESCRIPTION OF NETBIOS TIMERS**
ACKNOWLEDGEMENT TIMER - T2	The value for this timer specifies the delay that should occur before acknowledging a received frame when the number of maximum frames sent is less than the configured maximum The NetBIOS default value for this timer is 200 milliseconds. Increase this setting to 2,000 milliseconds.

SRVHEURISTICS

For the LAN Server machines that communicate with remote workstations you need to modify the SRVHEURISTICS parameter in the IBMLAN.INI file.

Locate the SRVHEURISTICS parameter in the IBMLAN.INI file and modify bit 15 from a 1 to any number between 2 and 8. This sets the timeout value to the maximum value of 127 seconds. If this does not improve performance, set the timeout value to to infinite by setting bit 15 to 9.

LAN Requester

For remote machines that are using LAN Requester you need to modify the WRKHEURISTICS and SESSTIMEOUT parameters in the IBMLAN.INI.

Locate the WRKHEURISTICS parameter in the IBMLAN.INI and change bits 11, 12, and 13 to 0.

Locate the SESSTIMEOUT parameter in the IBMLAN.INI file and increase this value from 45 to 300 seconds to prevent a LAN server session from timing out.

DOS LAN REQUESTER

For remote Windows workstations you need to make changes to the DOSLAN.INI file in the DOSLAN directory. You will need to add the following statements to the DOSLAN.INI file.

```
/NMS:3 /NVS:2 /API
```

Set the /NBS (network buffer size) to match the sizereqbuf parameter in the IBMLAN\IBMLAN.INI file. For example if the value of sizereqbuf is 4096 then set the /NBS parameter in the DOSLAN.INI to

```
/NBS:4k
```

Change the /BBS (big buffer size) parameter so that it is 1K larger than the /NBS parameter.

Change the fourth character in the /WKS (DLR heuristics) parameter to 0 and the last character to 1.

Communications Manager/2

If you are using CM/2 you need to ensure that the IEEE 802.2 driver has been added to your protocol configuration. If you experience problems like sessions being dropped you may need to incresae the IEEE 802.2 session timers.

You can access the session timers by configuring MPTS or editing the \IBMCOM\PROTOCOL.INI

The IEEE 802.2 protocol has two types of timers: Group 1 and Group 2 timers. CM/2 generally uses the Group 1 timers. These timer values are multiples of a tick value. A timer tick for the Group 1 timers is around 200 milliseconds or 0.2 second. The default values for Ti, T1 and T2 are 255, 15 and 3 respectively. That equates to approximately 50, 3 and 0.6 seconds respectively.

When you have a low speed remote link you should set the timers to:

- Ti=255 - inactivity timer, approximately 52 seconds
- T1=40 - response timer, approximately 10 seconds
- T2=2 - acknowledgement timer, approximately 0.28 seconds

The above values should reduce the likelihood of IEEE 802.2 applications timing out.

NetWare

If the remote workstations require access to a NetWare server ensure that the NetWare server has ROUTE.NLM loaded. This is required for the virtual bridge that the connection server creates.

If you intend to support clients using packet burst in this WAN environment the NetWare server must have the PBURST fix. For NetWare 3.11 you require PBURST.NLM. For NetWare 3.12 or 4.01 you require PBWANFIX.NLM which requires patchman.

On the OS/2 remote workstations running NetWare Requester 2.1 or later you will receive an REQ0815 error on startup. Ignore this message. Once the remote link is up you will be able to attach to the the NetWare servers.

On OS/2 remote workstations running NetWare Requester prior to 2.1 comment out the following line in your CONFIG.SYS:

```
RUN C:\NETWARE\NWDAEMON.EXE
```

Once you have done this restart your machine, dial the connection server and before attaching to a NetWare server type the following in at an OS/2 command line:

```
DETACH C:\NETWARE\NWDAEMON.EXE
```

You will need to do this each time you stop and restart your workstation.

7.13 Understanding Bridging and Filtering

In order to customize the Connection Server for a non-standard configuration it is important to understand how the bridging and filtering functions work. This section provides an overview of the bridging and filtering functions available. For a more complete discussion on bridging and filtering refer to the documentation referenced at the end of the chapter.

Remote Access Services Bridge Considerations

When setting up a Remote Access Services network, there are two points you should consider:

1. Coordinate segment numbers so there are no conflicts in the network.
2. Set the hop count appropriately to:

- Allow remote workstations to access other systems in the network
- Minimize the amount of unwanted traffic on the WAN link

Segment Numbers

The Remote Access Services bridges between two LANs. Generally, one LAN segment is a physical LAN segment (token-ring or Ethernet) and the other is the WAN, which is a virtual LAN segment. Segment numbers are used by bridges to route frames from one segment to another. All segments within a network should have a unique segment number.

It is important that when a Remote Access Services server is configured, the segment numbers used for the LAN and WAN segments are valid. In a small LAN environment where there are no interconnected segments (only one physical LAN segment exists), the LAN segment number can be any valid value. If the LAN environment is large, with many interconnected segments, then the segment number for the WAN and other remote LANs must be coordinated through a network administrator. Or, you can use OS2PING or CALLBRDG to be sure you are using a unique number. These are two utilities that ship with OS/2 Warp Server

Figure 258 shows remote LAN segments that are interconnected using Remote Access Services. Each segment within this network must have a unique segment number so that the Remote Access Services bridges can route the frames through the network.

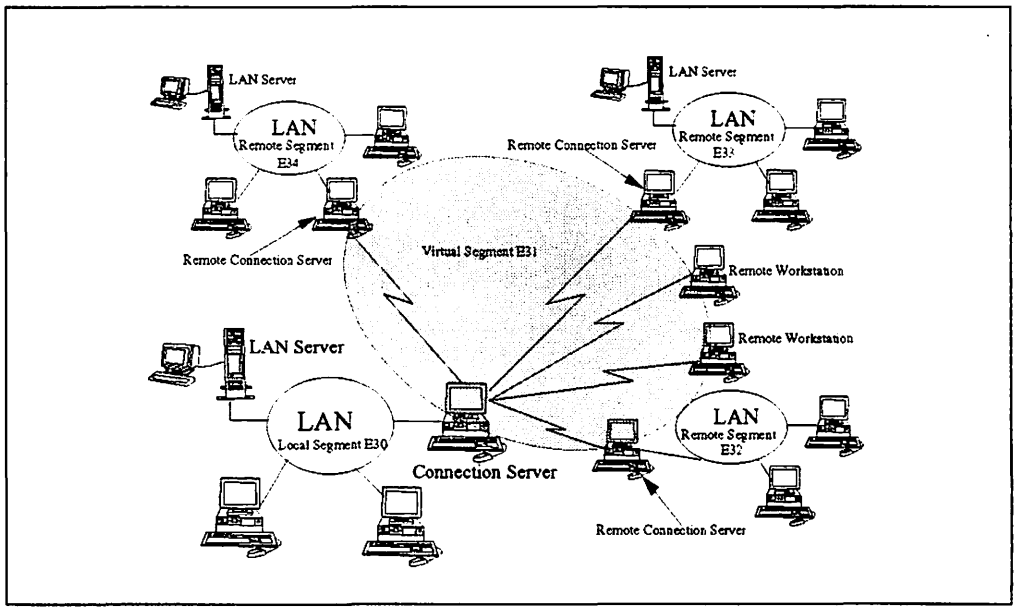


Figure 258. Interconnected LANs Using Remote Access Services

In this example, the network has five segments in total: one local LAN segment (E30), one WAN segment (E31), and three remote LAN segments (E32, E33, and E34). The following table shows how each Remote Access Services would have its segment numbers configured:

Table 68 (Page 1 of 2). Remote Access Services Segment Configuration

Connection Server	LAN Segment Number	WAN Segment Number

Table 68 (Page 2 of 2). Remote Access Services Segment Configuration		
Local	E30	E31
Remote 1	E32	E31
Remote 2	E33	E31
Remote 3	E34	E31

Hop Counts

A hop count is used by the Remote Access Services bridge and other LAN bridges to decide whether a frame should be discarded or not. The hop count limit indicates to a bridge the maximum number of bridges a broadcast frame can traverse before it is discarded by the bridge. For the IBM Token-Ring Network Bridge Program 1.x and the Remote Access Services bridge, the hop count affects both Single Route Broadcasts *and* All Routes Broadcasts. For the IBM Token-Ring Network Bridge Program 2.x, the hop count affects *only* All Routes Broadcasts.

The two sides of the bridge, either WAN-to-LAN or LAN-to-LAN, can have different values specified for the hop count limit. The value of (7,7) means that broadcast frames arriving on both sides of the bridge could have already traversed up to six bridges and will still be allowed to traverse this bridge. The number 7 represents the maximum number of bridges that can be traversed.

In a source routing bridge environment, as each bridge in a network is crossed, the bridge adds routing data to a routing information field. The maximum length of the routing information field is 16 bytes, which allows a maximum of 7 bridges to add their routing information (2 bytes per bridge, plus 2 bytes of control information).

In a large LAN environment where there are many LAN segments and bridges between a Remote Access Services and perhaps a host gateway, the hop count parameter can become critical to the effective operation of Remote Access Services. Let's take a look at Figure 259.

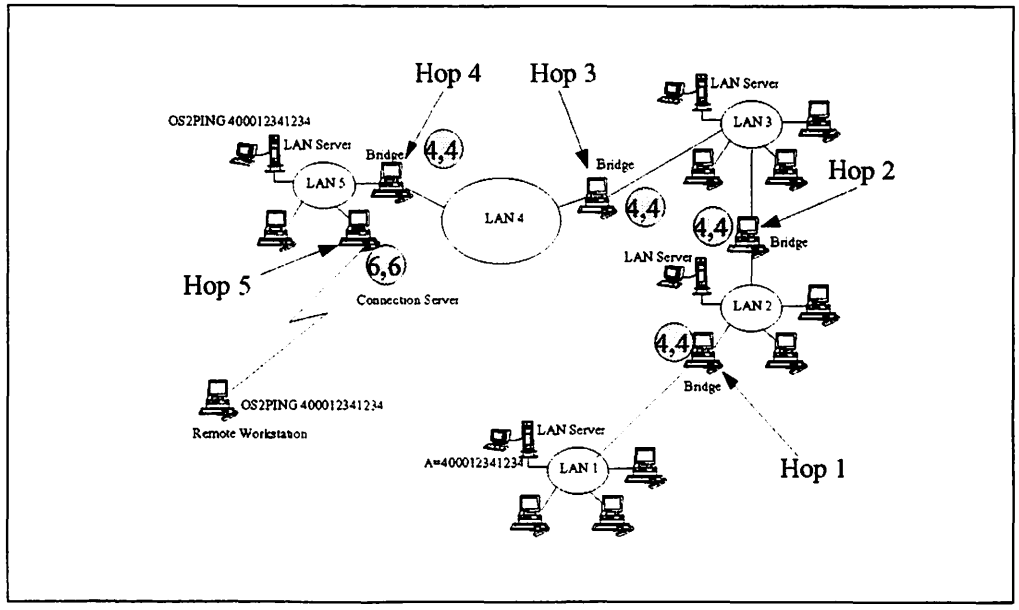


Figure 259. Setting Bridge Hop Counts

In Figure 259, the Remote Access Services on LAN 5 is four bridges away from the LAN Server on LAN 1. Each local bridge in this network has its hop count set to 4,4, thus any frame can traverse between any of the 5 LAN segments shown. When a Remote Access Services Remote Workstation is introduced and connects with the Remote Access Services, an additional bridge, and thus an additional hop, is introduced. Due to the additional hop in the network, it is not possible for the Remote Workstation to communicate with the LAN Server on LAN 1.

With Remote Access Services, if your network is large and contains many bridges and LAN segments, it is important that you understand the network topology.

There are two tradeoffs with setting the hop count on Remote Access Services:

- The hop count must be set large enough to enable the Remote Workstations to communicate with other devices in the network.
- A low hop count can assist with limiting the amount of unnecessary data on the slower WAN communications links.

If you set the hop count high, and there is a lot of broadcast traffic in the network, then the slow WAN link may be too busy transmitting unwanted broadcast traffic to be able to transmit information to and from the Remote Workstation. In this case, filtering has to be added to permit only certain adapters, NetBIOS names, or protocols to pass data over the WAN link.

If the hop count is set low, then there is less need to filter at the Remote Access Services. In fact setting the hop count low can assist or complement filtering for the purpose of reducing traffic over the WAN link. In some cases, such as with Communications Manager, it is possible to set the hop count on the Remote Access Services to 1, yet still be able to establish a connection with the host gateway.

When Communications Manager at the remote workstation first establishes a link with its gateway, it sends out an All Routes Broadcast to the gateway. As long as the bridges between the Remote Access Services and gateway have their hop count set high enough, the frame will reach the gateway. The gateway responds with a non-broadcast (direct) frame to the Remote Workstation. Because this frame is a non-broadcast frame, the bridges forward it through the network to the Remote Workstation. Even if the hop count on the Remote Access Services is set to 1, and the frame has passed over four bridges, the frame is still passed to the Remote Workstation by the Remote Access Services. The reason for this is that the bridge hop count only restricts broadcast frames.

Filtering

The Remote Access Services implements a bridge between a LAN segment and a WAN segment. As in any bridge, if filtering is not used the Remote Access Services forwards all LAN traffic that has routing information to the WAN segment and vice-versa. If the Remote Access Services is located on a busy LAN with large volumes of LAN traffic, the LAN side of the Remote Access Services tries to pass a large number of frames to the WAN side. Because the WAN side is usually much slower, it becomes overloaded, causing performance and connection problems.

In order to prevent these problems, the Remote Access Services allows you to control which frames can be passed between the LAN and the WAN segments. This is provided by the filtering feature. Two types of filtering are available:

- Automatic filtering

  In many cases this may be the only type of filtering needed. It provides an efficient way of preventing traffic from flooding the WAN link without requiring the user to go into the complex filter customization process. It also sets itself up specifically for each port. For example, if your Connection Server has eight ports servicing eight different remote workstations, Remote Access Services determines what type of filtering is required for each individual remote workstation and sets up eight filter criteria.

  Here are some examples of LAN traffic that the automatic filtering function filters:

  - Broadcast traffic
  - Traffic sent to functional addresses
  - Traffic sent to Ethernet multicast addresses or token-ring group addresses
  - Traffic with routing information addressed to stations that are not on the WAN segment

  Automatic filtering works for *most* NDIS-compliant protocols supported by Remote Access Services. Therefore, it can be used for most applications and LAN environments.

- Customized filtering

  The customized filtering feature provides a manual, more advanced way to control traffic flow through the bridge. Like automatic filtering it allows you to filter frames coming from the LAN side, but adds the capability to filter frames coming from the WAN side as well.

  Customized filtering, however, applies to all ports on the Connection Server. For example, if your Connection Server has eight ports servicing eight different remote workstations, any filtering you set up will be used for all of the remote workstations.

  With customized filtering, you must specify what will be filtered using panels in the Remote Access Services notebook. The connection server bridge supports the following filter types:

  - Source addresses
  - Range of source addresses
  - Bit mask destination address
  - Service Access Point (SAP)
  - NetBIOS names

Note: You can combine the two types of filtering. It is important to remember, however, that customized filtering will apply to all ports on the Connection Server (in addition to any automatic filtering).

It is highly recommended that you use filtering to reduce the amount of traffic on your Remote Access Services WAN connections. In most cases, LAN filtering is required in order for Remote Access Services to be effective. Filtering can also

be used to obtain a primary level of security by limiting access to resources on the LAN.

The recommendation is to always use some type of filtering (either automatic or customized) in order to improve connection reliability, performance and security.

7.14 PIF Files for Uncertified Modems

A Product Information File (PIF) is used to initialize a modem. The PIF file contains all needed string information and configuration values for your modem.

To set up a modem, initialization strings are needed. A modem initialization string is an AT command string passed to the modem when Remote Access Services server or requester is first started. The initialization string is used to configure and optimize the modem for use with Remote Access Services The PIF file has two parameters that are used to initialize the modem, `Initialization1` and `Initialization2`.

If you have a modem that is not supported, and you cannot get it to work using another supported modem type, it is usually because the initialization string is incompatible. There are a number of parameters that may need to be modified in a new modem PIF file. To help you, the CFMODEM utility is shipped with OS/2 Warp Server.

The CFMODEM utility is a small application to modify and create PIF files. This graphical utility should help you to create the needed PIF files for unlisted modems.

To create and modify modem strings and Remote Access Services PIF files, you need to have some technical knowledge on modems. Also you need to refer to your modem manual to find the correct commands.

The CFMODEM utility is normally installed from diskette 4 of the diskettes. To install from the OS/2 Warp Server CD-ROM, type the following commands:

```
X:\CID\SERVER\LDCS\LO319A4\INSTAPPL X:\CID\SERVER\LDCS\LO319A4\ Y:
```

Where

`X:` is your CD-ROM drive letter (which can be a redirected drive across a LAN as well)

`y:` is the target drive which contains the Remote Access Services (WAL) directory

The CFMODEM files are unpacked and copied to your WAL directory.

Note: The INSTAPPL utility installs the CALLBRDG applet also.

To develop a PIF file, start the CFMODEM utility from your desktop or, if you haven't added it to your desktop, from the command prompt. The utility will lead you through a series of panels, asking questions about the commands used by your modem. For further, more detailed information on using the CFMODEM utility, please refer to the *IBM LAN Distance Version 1.1 Installation and Customization Guide* or the *IBM LAN Distance Advanced Guide*.

7.15 Additional Information

- *IBM LAN Distance Advanced Guide Version 1.1* (S52G-8394-00), included in the OS/2 Warp Server package. This is both an administrative guide and a complete configuration guide for the Remote Access Services and the Remote Access Services client.
- *IBM LAN Distance Remote Guide Version1.1* (S52G-8393-00), included in the Remote Access Services package. This is a reference guide for Remote Access Services workstation users and focuses on using an asynchronous, switched line connection for remote access to a LAN.
- *IBM LAN Distance Version 1.1 Configuration and Customization Guide* (GG24-4158-01). This document is not included in the package. This document describes the IBM LAN Distance 1.1 product. It provides information on how to set up and customize LAN Distance in a simple stand-alone workgroup LAN environment. It also includes customization tips for supporting more complex configurations, multiprotocol application requirements for remote workstations, filtering techniques, and security.

Appendix A. Remote Access Services Internal Architecture

This appendix includes some information on the internal design and architecture of the Remote Access Services. You do not require a detailed understanding of the internal structure of the Remote Access Services to install and use it. The information presented here can prove valuable to people who are using Remote Access Services in an advanced environment.

A.1 Remote Access Services and ANDIS

Remote Access Services is based on an extended version of NDIS 2.0.1 called Advanced NDIS or ANDIS. The extensions defined by ANDIS provide support for communications environments and hardware outside the traditional token-ring or Ethernet LAN. ANDIS provides two basic functions beyond that of NDIS:

- Support for non-LAN networks such as asynchronous, synchronous, ISDN, X.25, and wireless connectivities

  ANDIS provides the ability to send LAN frames across these links and thus enable devices in the wide area network (WAN) to be participating members of the LAN.

  In fact, with ANDIS it is possible to develop protocol stacks that send many types of data, other than LAN specific frames, such as voice and image.

- Connection management

  In a LAN environment, as shown in Figure 260, the LAN-attached devices are always connected via their LAN adapters, cabling and other LAN hardware. Communication between two devices can occur at any time, and it is only necessary for one device to send data to the other.

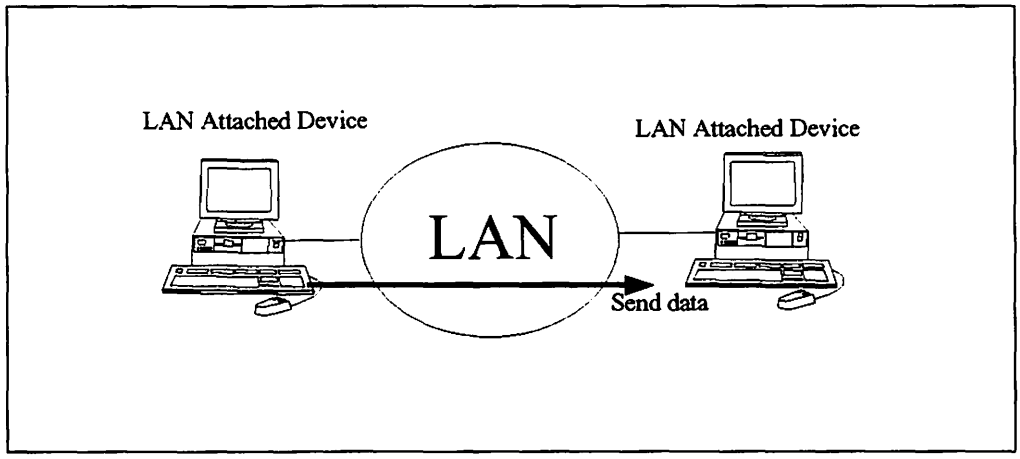


Figure 260. Simple LAN Communications

In Figure 261 on page 366, we can see that two people cannot communicate until a phone connection is made. It is the responsibility of either person to establish this connection (make the phone call). Once the connection is made, either person can speak to the other via this communications link.

© Copyright IBM Corp. 1996

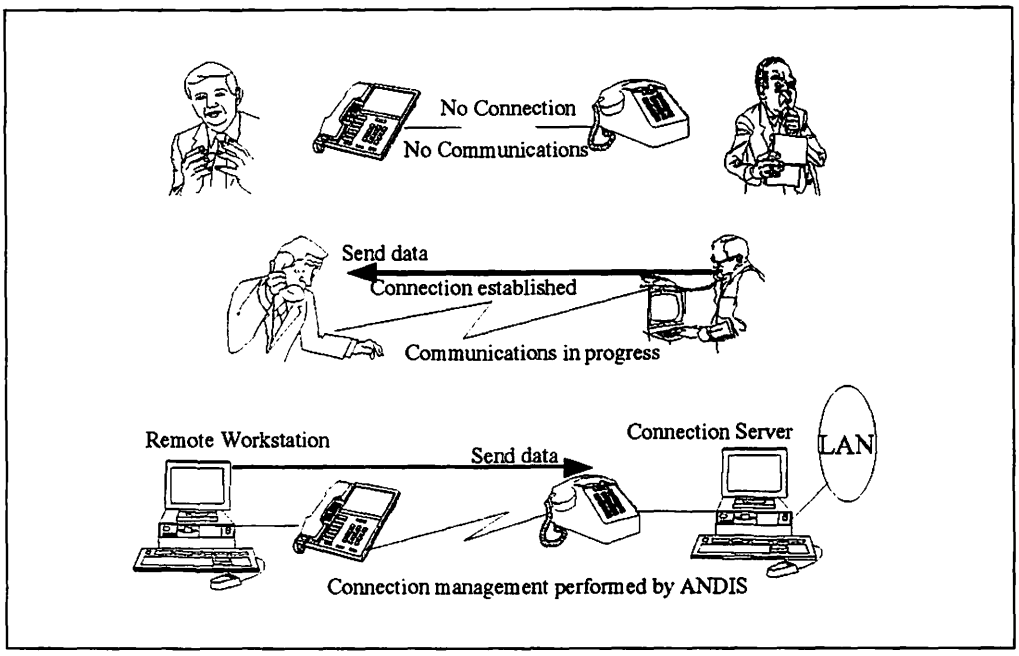


Figure 261. WAN Connection Management

In a standard LAN environment, as shown in Figure 260 on page 365, the physical connection always exists; thus, there is no need to establish this connection. With the ANDIS extensions to NDIS, the connection between the two remote workstations can be established. The ability to make these connections is called *connection management*.

A.2 ANDIS Connection Request Flows

In order to support LAN applications and protocols over non-LAN connections, the ANDIS architecture has added a number of new components to NDIS. These components include:

- Connection Manager
- Port Connection Managers
- ANDIS MACs
- Virtual LAN (VLAN)

More information on each of these components is presented in section "Remote Access Services Component Architecture" on page 368. Figure 262 on page 367 presents a high-level look at how an application would request a connection and how the ANDIS components work to manage this request and establish the communications link.

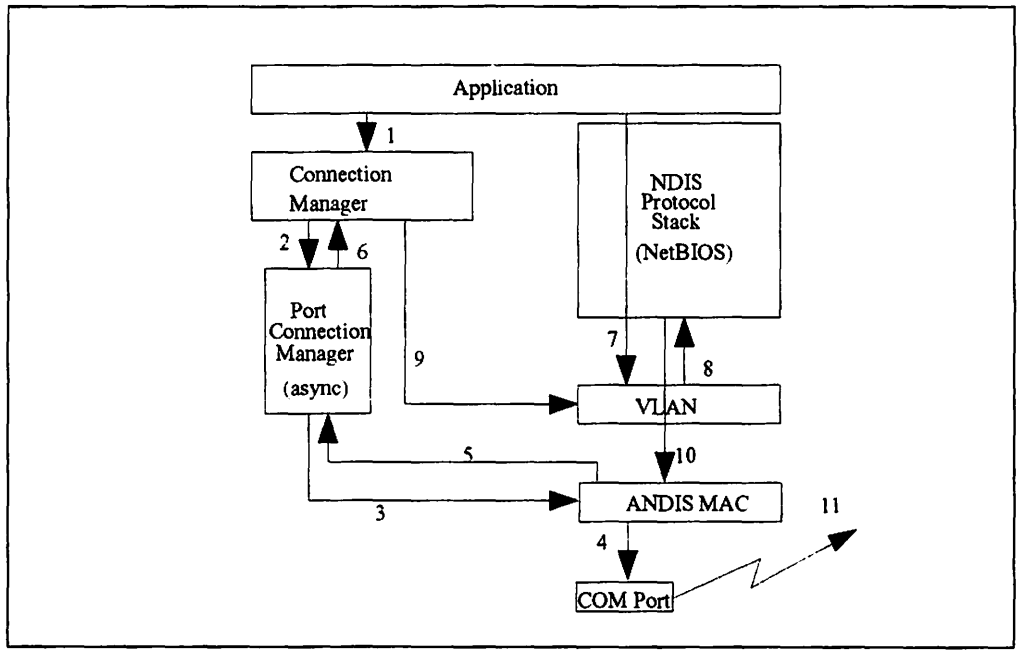


Figure 262. ANDIS Connection Request Flows

1. The application requests that a connection be made.
2. The Connection Manager passes this request to the appropriate Port Connection Manager for that connection type.
3. The Port Connection Manager creates the appropriate connection command and passes it to the ANDIS MAC driver.
4. The ANDIS MAC driver passes the command to the physical hardware.
5. The Port Connection Manager monitors the hardware via the ANDIS MAC driver and waits for the connection to be established.
6. After the connection has been established, the Port Connection Manager informs the Connection Manager.
7. The application makes calls to the protocol driver in an attempt to transmit data on the physical link.
8. The VLAN driver has not been informed that the link is available, so it returns an *Out of resources* error back to the protocol driver.
9. The Connection Manager informs the VLAN driver that the connection has been established.
10. The VLAN driver dynamically binds to the ANDIS MAC driver.
11. Data is transmitted over the newly established connection.

If the connection fails, the following occurs:

1. The Port Connection Manager monitors the connection (5) and notifies the Connection Manager of the failure (6).
2. The Connection Manager notifies the VLAN driver (9).
3. The VLAN driver dynamically unbinds from the ANDIS MAC driver (10) and returns an error to the protocol driver (8).

Remote Access Services Component Architecture

This section provides a discussion of the Remote Access Services components and an overview of the ANDIS extensions to NDIS. A strong understanding of NDIS is assumed in this discussion as no explanation of the standard NDIS environment is provided within this document.

Refer to the online *LAN Adapter and Protocol Support* manual for an explanation of NDIS.

Figure 263 shows an overview of the extensions to the NDIS architecture that ANDIS provides.

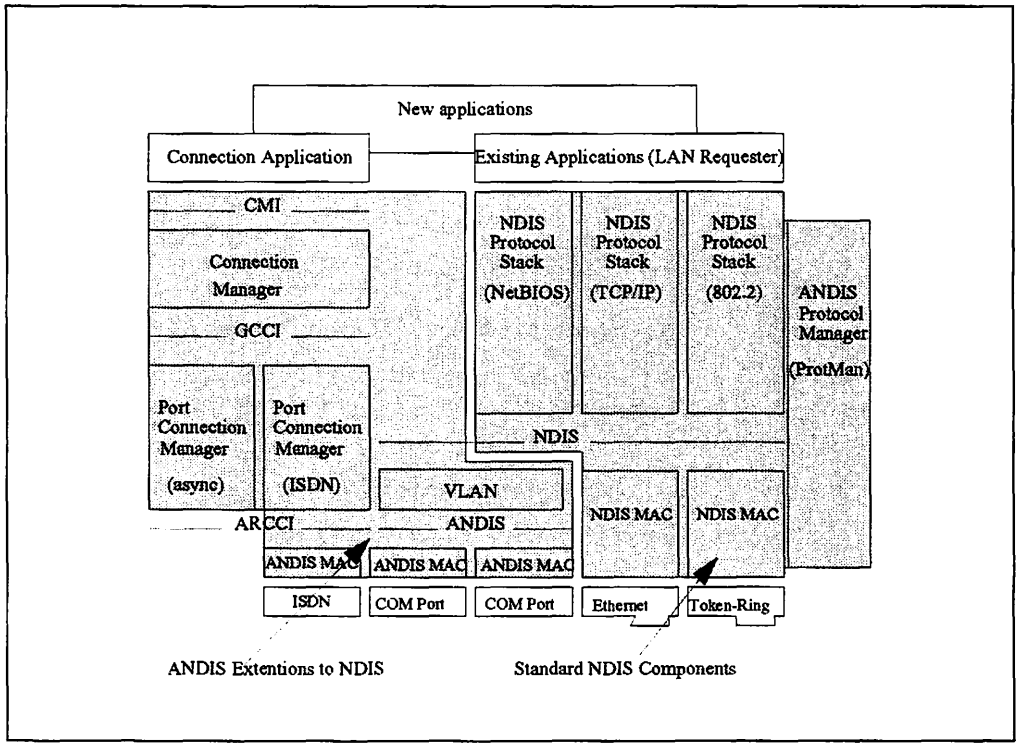


Figure 263. ANDIS Architecture Overview

The ANDIS architecture is a extension of the existing NDIS architecture. These extensions allow the support of different types of networks, connectivities, and protocols. Therefore, in addition to the basic NDIS components of MACs, Protocol Drivers (PDs), and the NDIS Protocol Manager (ProtMan) there are a number of new components:

- Connection Manager

  The Connection Manager is the common focal point for all *managed connections*. The Connection Manager maintains the status and other information about all the known connections.

  The Connection Manager has an upper-level interface, called the Connection Management Interface (CMI), that allows applications to activate, use and deactivate various types of connections. Another interface, called the Generalized Call Control Interface (GCCI), is used by the Connection Manager to communicate with the Port Connection Managers. The Port Connection Managers actually perform the low-level connection management.

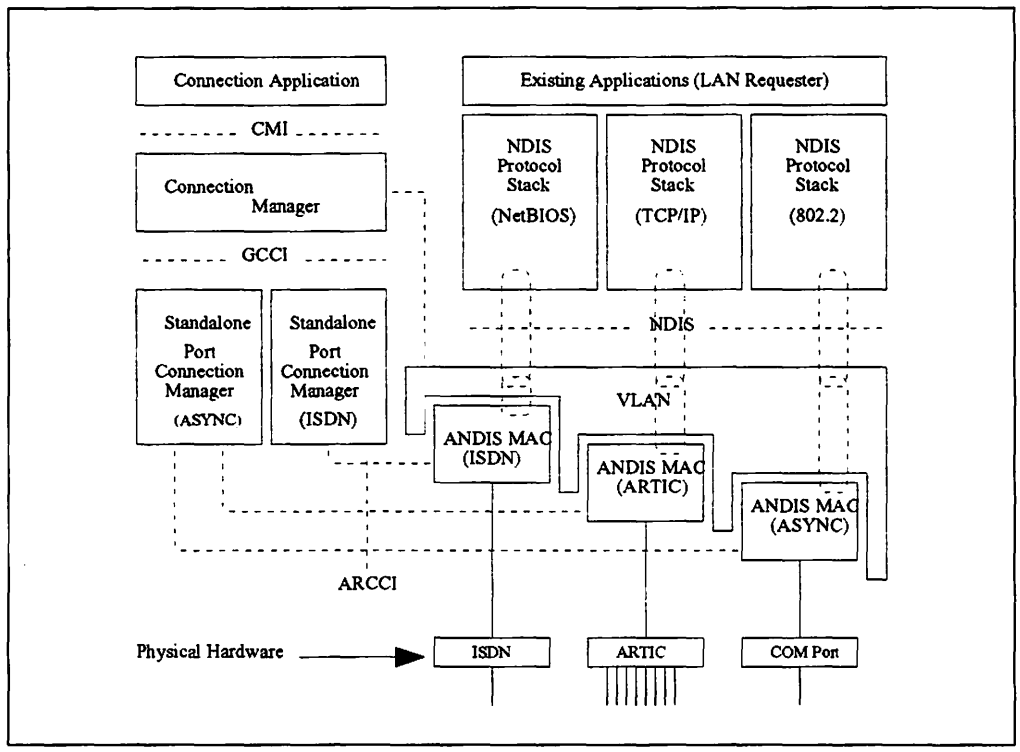


Figure 264. ANDIS Architecture Overview - Connection Manager

Figure 264 shows that the Connection Manager works with the Port Connection Managers to establish the physical connections. Once the physical connections have been established, the Connection Manager informs the VLAN and the connection application that the port connection is available. The VLAN then binds to the ANDIS MAC (see the description of the ANDIS MAC on page 371).

In summary, the Connection Manager provides a single interface to upper level applications. The Connection Manager then monitors and manages all connections established via the Port Connection Managers and informs the VLAN when a port connection is available.

- Port Connection Manager

  The Port Connection Managers (PCMs) are the entities that actually manage the ports or channels directly under their control. PCMs support specific types of connections such as asynchronous, ISDN, and X.25. A different PCM is required for each type of connection since each has its own form of connection management. In a dial-up asynchronous environment for example, the PCM is responsible for building the appropriate modem setup string and dial string for the modem being used, and then passing this to the modem that dials the remote system and makes the connection. Once the connection is made, the Connection Manager monitors it.

  There are two types of Port Connection Managers:

  1. Stand-alone PCMs

     A stand-alone PCM is connection specific and has a lower-layer interface called the ANDIS Real-time Connection Control Interface (ARCCI). This lower layer interface is the interface between the PCMs and the ANDIS MACs (see Figure 265 on page 370). The PCM uses this interface to pass connection and other management commands to the hardware via

the ANDIS MACs. An example of a stand-alone PCM is the ASYNC PCM shipped with Remote Access Services.

All stand-alone PCMs must *find* the MACs that need their type, or form, of connection management to operate. This is achieved by getting a list of MACs that support Port Connection Management from the ANDIS ProtMan, and then determining which ones need the PCM's specific form of connection control.

An example of stand-alone PCMs is shown in Figure 264 on page 369. Also shown in this example is that one PCM can work with multiple ANDIS MACs. In this example, the ASYNC PCM that establishes connections via asynchronous modems is used with both the COM port MACs and the ARTIC MACs. Although the physical hardware is quite different, both hardware types use the same modems and thus the same connection support must be provided. In the case of ISDN however, the hardware and the connection method are different.

2. Integrated PCM subsystems

   An integrated PCM subsystem contains both the PCM and the MACs required to support a specific piece of hardware and connection type in an integrated package. The PCM(s) and the MAC(s) act as a single system, with no formal external interface between the two. This integrated subsystem package is product specific. Integrated PCM subsystems would normally be shipped with OEM hardware where there is no requirement to externalize the PCM/MAC interface. An example of an integrated PCM is the PCM which supports the ISDN Co-processor/2.

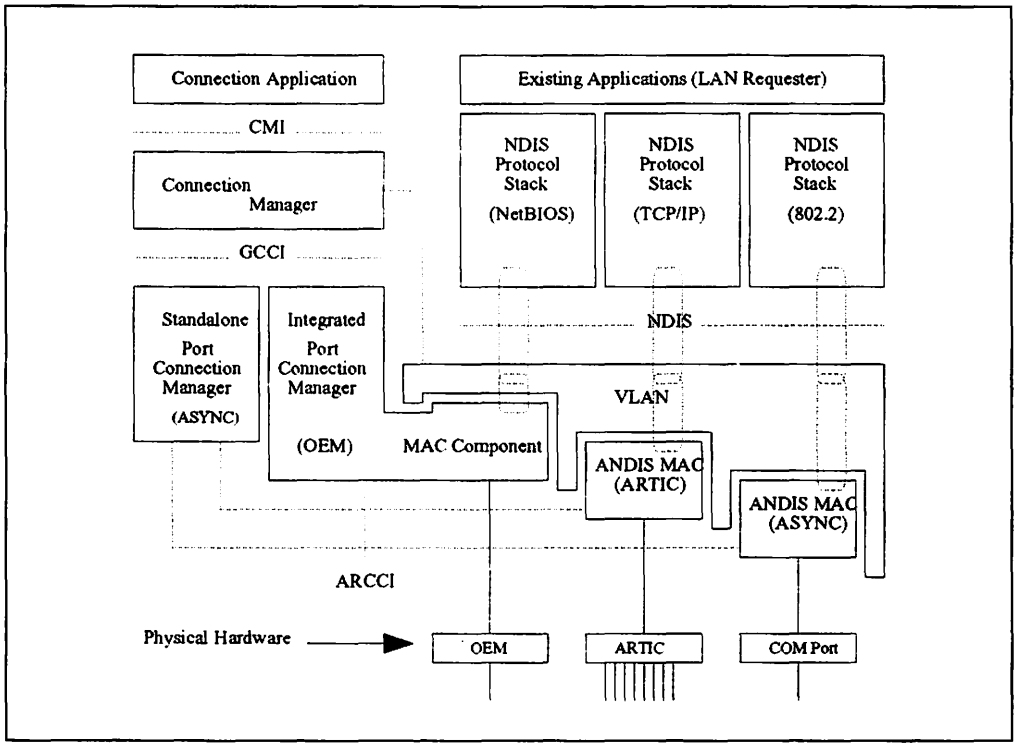


Figure 265. ANDIS Architecture Overview - Integrated Port Connection Manager

Figure 265 shows an example of an integrated PCM and the stand-alone PCM. Although the interface between the ANDIS MAC and the PCM is not externalized, an NDIS MAC must still exist within the integrated PCM.

A number of PCMs are supplied with Remote Access Services. These PCMs support asynchronous, synchronous, and ISDN. The signaling protocols that are used by the PCMs are industry standards for the particular connection type and include the following (this is a list of the *signaling protocols* and not the physical connection types):

Asynchronous	AT Command Set
Synchronous	V.25bis
ISDN	Q.921 Q.931

- ANDIS MACs

  Standard NDIS MAC drivers provide a standard interface to LAN hardware. This interface allows higher-level protocols, which build the LAN specific frames, to pass these frames and other command information to the LAN adapter. ANDIS extends the standard NDIS MAC functions to encompass connection management via an external or stand-alone PCM. ANDIS MACs, that require connection management and are not part of a specific integrated PCM subsystem, support ANDIS Connection Management Architecture (CMA) by implementing the ANDIS Real-time Connection Control Interface (ARCCI).

  Some ANDIS MACs support or manage media that is not protocol sensitive, such as analog and digital WANs. These MACs still support existing protocol drivers such as NetBIOS and TCP/IP, which generate LAN protocol specific frames such as 802.5 (token-ring) and 802.3 (Ethernet). The existing protocol drivers use standard NDIS commands to pass these frames and other command information to the new ANDIS MACs.

  For example: A NetBIOS protocol driver builds the appropriate 802.5 frame, passes this frame to the token-ring adapter MAC driver and issues a SEND command. By replacing the token-ring adapter MAC driver with an asynchronous ANDIS MAC driver, the frame would be sent across an asynchronous communications link. The device on the other end of the async communications link would receive this frame as asynchronous data. If an ANDIS MAC driver exists at the remote port, then the 802.5 frame is received from the line and passed back up to the standard NetBIOS protocol driver. This protocol driver would have no knowledge that the frame was transmitted across an asynchronous link.

- Virtual LAN (VLAN)

  VLAN is a new layer which sits between the standard NDIS protocol drivers and the ANDIS MACs. The VLAN emulates LAN types and routes frames between the WAN connection, protocol stacks, and the bridge (source routing for token-ring and transparent for Ethernet). The VLAN appears to the upper-layer protocol driver as a real LAN adapter. Thus, there would be a different VLAN for token-ring and Ethernet. The VLAN insulates the NDIS protocol drivers from the non-static characteristics of dynamic connections. The VLAN appears as standard MACs to the protocol drivers above and as surrogate protocol drivers to the ANDIS MACs.

  The VLAN works with the Connection Manager, ANDIS MACs and protocol drivers. If there is no communication connection established, then the VLAN blocks all data transmission between the protocol driver and the ANDIS MAC. In this case it returns a standard error back to the protocol driver, such as *Out of resources*, to indicate to the protocol driver that communication is not possible at this time. When a communication

connection is established, the Connection Manager informs the VLAN and the VLAN binds to the ANDIS MAC driver, thus allowing communications to progress. See Figure 264 on page 369 and Figure 265 on page 370.

The ANDIS MAC layer allows standard NDIS protocol drivers to operate unchanged over various types of connections by hiding the connection type specifics from the NDIS MAC interface.

- Bridge

  The Remote Access Services bridge functions as a source-routing bridge in the token-ring environment and a transparent bridge in the Ethernet environment.

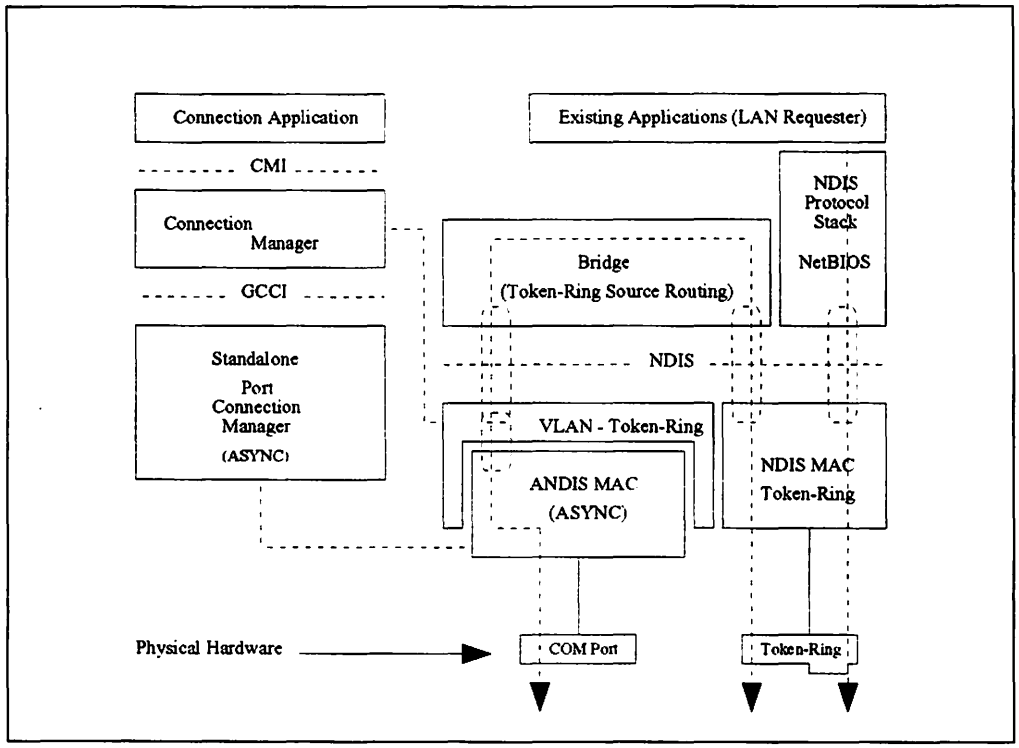


Figure 266. ANDIS Architecture Overview - Source Routing Bridge

As shown in Figure 266 a source routing bridge, is used by the Remote Access Services connection server to route LAN traffic to and from the WAN and LAN. Also shown in this figure, is that other NDIS protocols can still exist and use a MAC concurrently.

With Ethernet and transparent bridging, other NDIS protocols *cannot* use a MAC concurrently. Since there is no routing information in the Ethernet frames, the Remote Access Services bridge must look at *every* frame. All frames on the LAN are copied, including frames not destined for the workstation. Other NDIS protocols do not operate properly in this environment.

- ANDIS Protocol Manager (ProtMan)

  The NDIS Protocol Manager reads in configuration information from the PROTOCOL.INI file and uses this to bind, or connect, the NDIS protocol stacks to the NDIS MAC drivers. Once the appropriate protocol stacks and MAC drivers are bound, the Protocol Manager is no longer used.

ANDIS adds additional function to the NDIS Protocol Manager to include the ability to bind the Connection Manager, Port Connection Managers, and ANDIS MACs together as required. Thus, there is additional configuration information required in PROTOCOL.INI to accomplish this.

A.3 Relationship Between a Remote Workstation and the Connection Server

Figure 267 shows the relationship between a Remote Workstation, the connection server, the LAN, and other LAN-attached devices in a token-ring environment. The diagram also shows how the different ANDIS components are used on the Remote Workstation and connection server. The environment shown is rather simple as many other combinations of protocols, LANs, and applications can be supported by Remote Access Services.

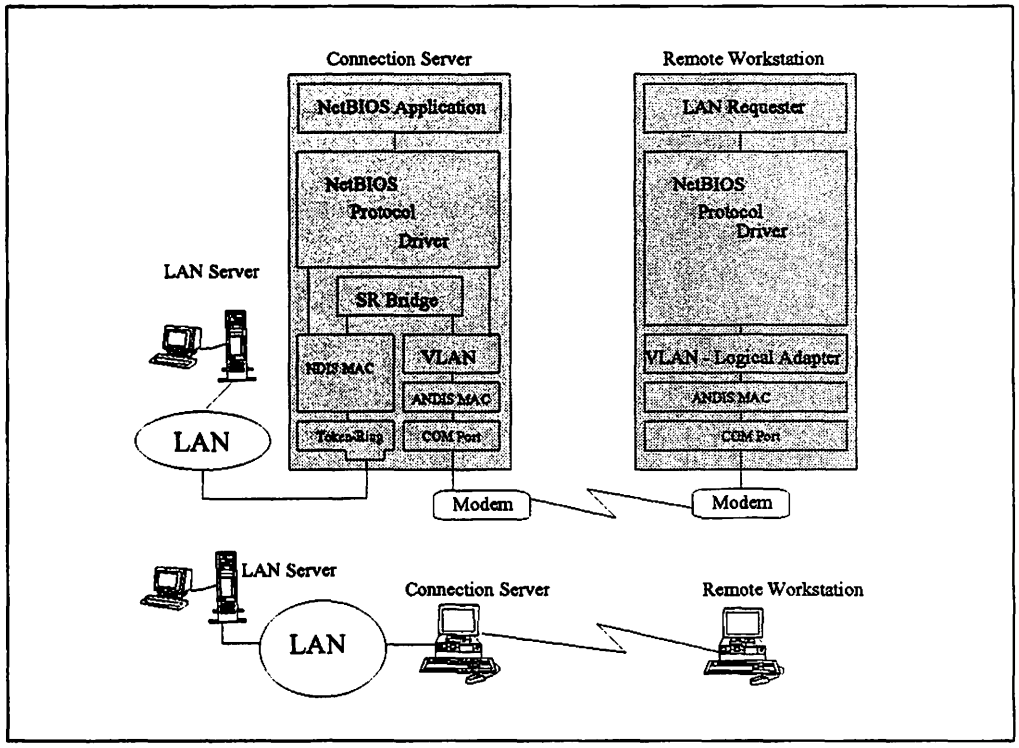


Figure 267. Connection Server and Remote Workstation Relationship - Token-Ring

In this diagram only the ANDIS components used by Remote Access Services for communications (not establishing the connection) are shown. The Connection Manager and Port Connection Managers as described in section "Remote Access Services Component Architecture" on page 368 are not shown.

On the Remote Workstation, LAN requester is running and using the NetBIOS protocol. Although only NetBIOS is shown in this diagram, any NDIS protocol driver can be supported. The NetBIOS protocol is then bound to the virtual LAN adapter or VLAN driver. After the connection between the Remote Workstation and the connection server has been established, the Connection Manager (not shown) allows the VLAN driver to dynamically bind to the MAC driver. LAN Requester requests can now flow across the link shown as if they were directly attached to the LAN.

On a token-ring LAN, the connection server has a standard MAC driver loaded for the token-ring adapter, as well as the ANDIS drivers for the WAN

communications. In addition, a source routing bridge module has been added. This bridge routes frames to and from the Remote Workstation (WAN) and the LAN. The Remote Access Services bridge is key to the function of the connection server enabling LAN frames to flow between the LAN and Remote Workstation in the WAN.

Note: On the connection server, the VLAN driver must match the physical LAN to which the connection server is to be attached. In the case of token-ring, the VLAN must support token-ring frames. Also, the Remote Workstation must send the correct frames which in this case are token-ring frames.

Also shown in Figure 267 on page 373 is the NetBIOS protocol driver on the connection server. *The NetBIOS protocol stack is always required on both connection server and Remote Workstation for DOS and OS/2 even if no other NetBIOS application is used* because Remote Access Services uses NetBIOS itself for internal purposes. This is the reason why the Remote Access Services product provides the NetBIOS protocols on the LAPS disk for the OS/2 product and provides also its own DXMJ0MOD.SYS for the MS Windows version. Use this version of DXMJ0MOD.SYS, because it contains the latest fixes to the NetBIOS stack.

Figure 268 shows the relationship between a Remote Workstation, the connection server, the LAN, and other LAN-attached devices in an Ethernet environment.

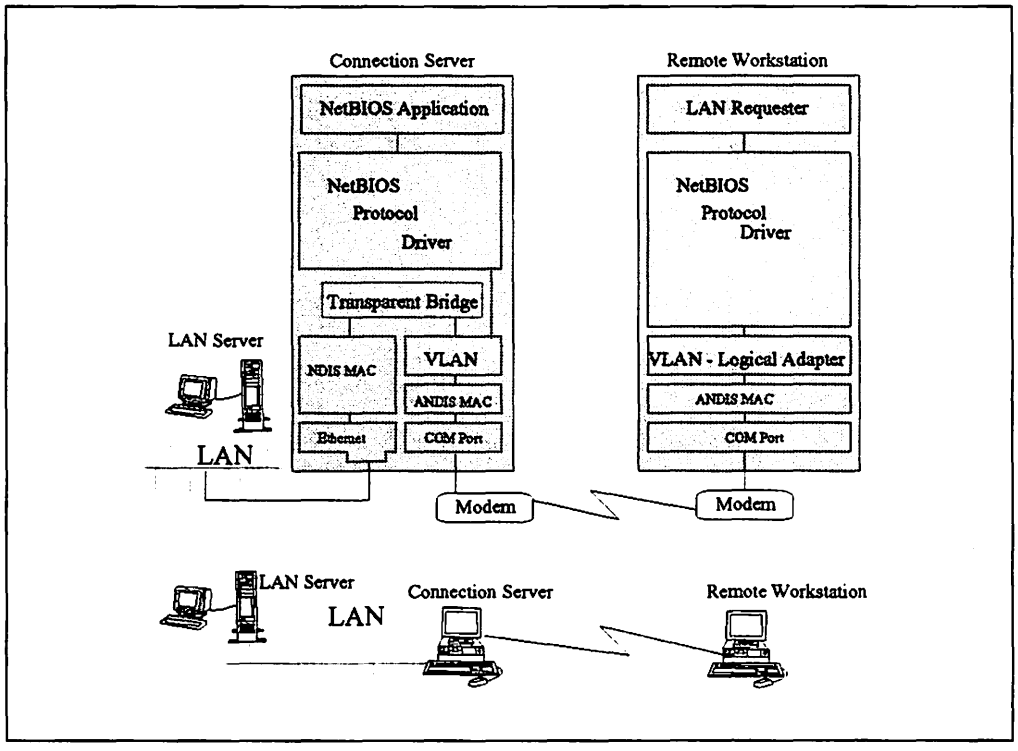


Figure 268. Connection Server and Remote Workstation Relationship - Ethernet

When the LAN is Ethernet, the connection server uses transparent bridging. Because there is no routing information included in the Ethernet frames, the Remote Access Services bridge must check the source and destination address of every frame to compare against entries in the bridge routing table. To do this, Remote Access Services sets the adapter to *promiscuous mode*, meaning that the Ethernet adapter receives all frames on the LAN, including frames not

destined for this workstation. For this reason, only the transparent bridge is allowed to bind to the Ethernet NDIS MAC. Other protocols can bind to the VLAN protocol, however.

Note: In the case of Etherent, the VLAN in the connection server and the VLAN in the Remote Workstation must be compatible with Ethernet frames and protocols. The VLAN is a different piece of code in Remote Access Services for Ethernet and token-ring.

List of Abbreviations

ADSM	ADSTAR Distributed Storage Manager	***IETF***	Internet Engineering Task Force
DDNS	Dynamic Domain Name Server	***IBM***	International Business Machines Corporation
DHCP	Dynamic Host Configuration Protocol	***ITSO***	International Technical Support Organization
DCDB	Domain Control Database	***NBNS***	NetBIOS Name Server
DLS	DOS LAN Services		

© Copyright IBM Corp. 1996

Index

A

abbreviations 377
Access Control 41
accounts, user 332
acronyms 377
Adapter and Protocol Services
  adapter and protocol support 126
  applets 154
  BALANCE parameter 149
  Bindings statements, PROTOCOL.INI 130
  configuration 142
  Converged Stack 132
  DDNS client 125
  DHCP client 125
  IEEE 802.2 protocol 126, 133
  IEEE 802.2 RAM usage 141
  installation 133
  IPX over NDIS 158
  IPX/SPX over NDIS support 126, 133
  LAN Adapter and Protocol Support 126
  LAPS 126
  limit of adapters 149
  MAPNAME utility 157, 267, 268
  memory requirements 137
  MPTS 131
  multiple protocol support 129
  native Sockets services 133
  native transport 132
  NB64K utility 154
  NBJDSTAT utility 154
  NDIS 127
  NetBEUI RAM usage 137
  NETBIND process 131
  NetBIOS over IPX support 126
  NetBIOS over TCP/IP 126
  NetBIOS protocol 126, 133
  NetBIOS RAM usage 139
  NetBIOS Socket access 147
  NETPING utility 156
  NetWare NetBIOS Emulation 159
  network protocols 126
  New Features 125
  non-native Sockets services 133
  non-native transport 132
  ODI2NDI driver 158
  PROTOCOL.INI 130
  publications 166
  removing 166
  removing TCPBEUI 275
  SIDEBAND parameter 149
  Socket/MPTS 144
  supplied adapter drivers 133
  TCP/IP protocol 126, 133
  TCP/IP protocol capability 263
Adapter and Protocol Services *(continued)*
  TCP/IP Socket access 144
  TCPBEUI 125, 260
  TCPBEUI RAM usage 138
  Virtual Device Drivers 128, 165
adapter and protocol support, see Adapter and Protocol Services
administrator - Remote Access Services 332
advanced NDIS 365
AF_INET 132
AF_INET address family 131
AF_NB 132
AF_NB address family 131
AF_OS2 132
AF_OS2 address family 131
ANDIS 365
  architecture 368
  components 366
  MACs 371
  protocol manager 372
ANDIS MACs 366
Answer Modes 303
AnyNet
  AnyNet product family 132
  AnyNet/2 133
  native Sockets services 133
  native transport 132
  non-native Sockets services 133
  non-native transport 132
AnyNet product family, see AnyNet
architecture 365
ARP program 263
Asyncronous 309

B

BALANCE parameter, see Adapter and Protocol Services
Bindings statements, PROTOCOL.INI 130
Bit mask 362
BootP, see TCP/IP Services
Bootstrap Protocol, see TCP/IP Services
Bridge 298, 358
bridge, Remote Access Services 372
Bridging Adapter 301

C

callback 337
Capture 37
certificate, server 335
CFMODEM 363
CMADD 354
CMBACKUP 354

© Copyright IBM Corp. 1996

CMPRINT 354
connection manager 366, 368
Connection Server 281, 287
  relationship with Remote Workstation 373
Converged Stack, see Adapter and Protocol Services
Customized filtering 362

D

Data Encryption Standard, see Cryptography
database, user accounts 332
DDNS
  BootP reply message 239
  BootP request message 239
  complex scenario 237
  creating a new DDNS configuration 223
  DDNS client 125, 217, 227, 228
  DDNS Client Configuration Program 231
  DDNS client to server interaction 217
  DDNS database 219, 227
  DDNS message format 218
  DDNS message header 219
  DDNS resource records 220
  DDNS server 168, 217, 227
  DDNS server configuration 222
  DDNS transaction 219
  DDNS update message 219, 234, 238
  DDNSZONE command 224, 226
  DHCP server 217
  DHCPSD.DAT file 211
  DNS security extensions 216
  DNS security functions 214
  domain name message format 218
  Domain Name System 216
  dynamic DNS protocol 216
  dynamic pre-secured DDNS server 222
  dynamic secure DDNS server operation 222
  KEY resource record 220
  NAMED program 227
  NAMED.BT file 223, 226, 235
  NAMED.DOM file 223, 226, 235
  NAMED.REV file 223, 226, 235
  NSLOOKUP program 227
  NSSIG program 227
  NSUPDATE program 227
  OEM compatibility 239
  OS/2 client installation 228
  primary DDNS client 218
  primary DDNS database 218
  primary DDNS security 218
  primary DDNS server 218
  primary DHCP server 218
  server installation 171
  SIG resource record 221
  simple scenario 233
  static DDNS server operation 222
  supply host name 231
  SYSLOG.CNF file 226, 236
  using multiple servers 239
DDNS Client Configuration Program, see DDNS
DDNSZONE command 224, 226
Deinstalling Remote Access Services 322
Deinstalling Remote Access Services Clients 322
DES, see Cryptography
DHCP
  BootP 199
  BootP message format 203
  BootP realy agent 200
  BootP relay agent 199
  BootP reply message 239
  BootP request message 239
  Bootstrap Protocol 199
  BOUND state 200
  complex scenario 237
  connecting to a Windows NT server 241
  connecting Windows 95 clients 240
  connecting Windows NT clients 239
  DHCP client 125, 146, 199, 212, 228
  DHCP Client Monitor 229
  DHCP client state transition diagram 202
  DHCP message fields 203
  DHCP message format 202
  DHCP message types 202
  DHCP options 204
  DHCP server 168, 200, 205, 209, 210, 211, 212, 217
  DHCP server automatic operation 206
  DHCP server class configuration 207
  DHCP server client configuration 207
  DHCP server configuration 205, 209
  DHCP server configuration file 209
  DHCP server configuration program 206, 209
  DHCP server dynamic operation 206
  DHCP server log file 211
  DHCP server manual operation 206
  DHCP server network configuration 207
  DHCP server options configuration 207
  DHCP server parameters 210
  DHCP server status files 212
  DHCP server subnet configuration 207
  DHCP server vendor configuration 207
  DHCPACK message 200, 201, 202, 212, 234, 238
  DHCPC.AR file 212
  DHCPC.CR file 212
  DHCPC.DB file 233
  DHCPCD.CFG file 229, 236
  DHCPCD.EXE program 228
  DHCPCD.LOG file 232
  DHCPDECLINE message 200, 203
  DHCPDISCOVER message 199, 200, 201, 202, 234, 238
  DHCPIBM.CMD file 212, 231
  DHCPINFORM message 201, 203
  DHCPNACK message 200, 203
  DHCPOFFER message 200, 201, 202, 234, 238
  DHCPRELEASE message 201, 203
  DHCPREQUEST message 200, 201, 202, 212, 234, 238

DHCP *(continued)*
DHCPSD program 210
DHCPSD.CFG file 209, 235
DHCPSD.DAT file 211
DHCPSD.LOG file 211
external configuration 201
INIT state 200, 201
initialization and acquisition process 199
KEY resource record format 220
lease timers 201
NSUPDATE command 231
OEM compatibility 239
OS/2 client installation 228
primary DHCP server 218
rebinding and rebooting processes 201
REBINDING state 201
RENEWING state 201
server installation 171
SIG resource record format 221
simple scenario 233
site-specific options 198, 205, 212, 231
supply host name 231
updateDNS string 231
using multiple servers 239
DHCP Client Monitor, see DHCP
DHCPC.DB file 233
DHCPCD.CFG file 229, 236
DHCPCD.EXE program 228
DHCPCD.LOG file 232
DHCPIBM.CMD file 212, 231
DHCPS.AR file 212
DHCPS.CR file 212
DHCPSD program 210
DHCPSD.CFG file 209, 235
DHCPSD.DAT file 211
DHCPSD.LOG file 211
directed broadcast, see TCPBEUI
Domain Name System, see DDNS
Domain Nameserver, see TCP/IP Services and TCPBEUI
DOMAINSCOPE parameter, see TCPBEUI
DOS LAN Requester 357
Dynamic IP
BootP 197
BootP relay agent 199
BootP server 198
Bootstrap Protocol 197
complex scenario 237
connecting to a Windows NT server 241
connecting Windows 95 clients 240
connecting Windows NT clients 239
customer benefits 198
Dynamic Domain Name Services 198
Dynamic Host Configuration Protocol 198
introduction 197
objectives 198
OEM compatibility 239
OS/2 clients 228
Dynamic IP *(continued)*
simple scenario 233
system components 198
using multiple servers 239

E

encryption standards
authentication 214
Data Encryption Standard 215
DDNS server 214
DES 215
digital envelope 215
digital fingerprint 214
digital signature 214, 227
DNS security functions 214
encryption 214
hash function 214
introduction 214
MD5 algorithm 216
message digest 214
modulus 214
private exponent 215
private key 214, 215
public exponent 215
public key 214, 215
RSA encryption standard 214
secret key 214
encryption, see Cryptography
EXPLORE.INI file 196

F

Fault Tolerance
administration 9
drive mirroring 9
FIFO buffering 286
File and Print Sharing Services
386 HPFS startup diskette 9
access control profile 21, 23
Administration GUI 8, 19
aliases 19, 24
Audit Log Utility 8
client installation 28
command line 27
Configuration
current shares window 27
domain 10
double redirection 43
Error Log Utility 8
feature installation 12
Installation 10
LAN Services folder 7
Logging off 8
Logging on 7
logon assignments 19
NetWare Gateway 33
Network DDE and Clipboard 8
Network Messaging 8

File and Print Sharing Services *(continued)*
remote installation 29
resource definitions folder 20, 23
Ring 3 33
sharing directories 20
sharing printers 23
Starting the server 7
Tuning Assistant 8
WSTUNE.EXE parameters 18
Filtering 298
Filters 358

G

Gateway Services
File and Print Gateway 32
NetWare 33
NetWare Overview 33
Overview 33
Gopher, see TCP/IP Services
GOPHER.INI file 196

H

hash algorithm 332
Hop Count 358, 360
HOST program 263
HOSTNAME program 263
HOSTS file 181, 197
hosts file, see TCP/IP Services and TCPBEUI

I

IBM Internet Connection family, see TCP/IP Services
IBMLAN.INI 267
IEEE 802.2 RAM usage, see Adapter and Protocol Services
IFCONFIG program 228, 263, 274
Inactivity Threshold - Remote 323
Inactivity Timeout Feature 323
Inactivity Timer - Remote 323
INETCFG program 274
INETD super server daemon, see TCP/IP Services
INETD.LST file 197
Installation Considerations
RAID Machines 13
Installing Remote Access Services 287
integrated PCMs 370
internal architecture 365
Internet access, see TCP/IP Services
Internet server, see TCP/IP Services
IPFORMAT program 263
IPTRACE program 263
IPXNB driver, see IPXBEUI
ISDN 303, 305

K

key, password 332

L

LAN Adapter and Protocol Support, see Adapter and Protocol Services
LAN Distance 281
LAN Distance logical adapter 301
LAN Distance Messages 304
LAN segment filter criteria 301
LAN Server
Administration GUI 8
Audit Log Utility 8
Error Log Utility 8
LAN Services folder 7
Network Messaging 8
Starting the server 7
LANPDD.OS2 device driver 165
LANVDD.OS2 device driver 165
LAPS, see Adapter and Protocol Services
LDREMOVE 322
LM10 API, see NetBIOS
Logical LAN Distance Adapter 311
logon 333
specifying valid times 339
specifying valid workstations 339
LPR_PRINTER environment variable 189
LPR_SERVER environment variable 189
LPRMON program 46
LPRPORTD program 46, 189
LTSVCFG command 165

M

MACs
ANDIS 371
Map 37
MAPNAME utility, see Adapter and Protocol Services
MD5 algorithm, see Cryptography
message authentication codes 333
Modem Classes 309
Modems 363
MPTN
MPTN 132
Multiprotocol Transport Network architecture 132
MPTS, see Adapter and Protocol Services
MTU size 274
Multiple Lines 324
Multiprotocol Transport Network architecture, see MPTN

N

NAMECACHE parameter, see TCPBEUI
NAMED program 227
NAMED.BT file 223, 226, 235

NAMED.DOM file 223, 226, 235
NAMED.REV file 223, 226, 235
NAMESFILE parameter, see TCPBEUI
native Sockets services, see Adapter and Protocol Services and AnyNet
native transport, see Adapter and Protocol Services and AnyNet
NB30 API, see NetBIOS
NB64K utility, see Adapter and Protocol Services
NBJDSTAT utility, see Adapter and Protocol Services
NDIS 127, 128, 129, 135, 157
  multiple protocol support 129
  NETBIND process 128
  NETBIND.EXE 128
  network adapter driver 128
  network protocol driver 128
  PROTMAN.OS2 128
  Protocol Manager 128
  PROTOCOL.INI 128
Net Share 41
NET.CFG file 161
NetBEUI RAM usage, see Adapter and Protocol Services
NETBIND.EXE 128
NetBIOS 311
  limit of adapters 149
  LM10 API 149, 159, 261, 262
  NB30 API 149
  NetBEUI RAM usage 137
  NetBIOS RAM usage 139
  NetWare NetBIOS Emulation 159
  RFC encoded NetBIOS names 267
  TCPBEUI 125
  TCPBEUI RAM usage 138
NetBIOS Name Server
  NetBIOS Name resolution problem 259
NetBIOS names 362
NetBIOS over IPX
  coexistence 160
  configuration 161
  IPXNB driver 159
  limitations 165
  NetWare NetBIOS Emulation 159
  performance 165
  protocol stack 160
  sample files 163
NetBIOS over TCP/IP, see TCPBEUI
NetBIOS RAM usage, see Adapter and Protocol Services
NetBIOS Timers 356
  Acknowledgement Timer 356
  Inactibity Timer 356
  Response Timer 356
NETPING utility, see Adapter and Protocol Services
NETSTAT program 148, 263
NetWare - RAS 358
NetWare Gateway 33
NetWare NetBIOS Emulation, see IPXBEUI
NetWare Requester
Network DDE and Clipboard 8
Network Driver Interface Specification, see NDIS
Network File System, see TCP/IP Services
NewsReader/2, see TCP/IP Services
NFS, see TCP/IP Services
non-native Sockets services, see Adapter and Protocol Services and AnyNet
non-native transport, see Adapter and Protocol Services and AnyNet
nonce, definition 334
Nonswitched Lines 305
NR2.INI file 196
NSLOOKUP program 227
NSSIG program 227
NSUPDATE program 227

O

ODI 157
  Link Support Layer 157
  LSL 157
  MLID 157
  Multiple Link Interface driver 157
  NET.CFG file 157
  network protocol drivers 157
ODI2NDI driver, see Adapter and Protocol Services
Open Data-Link Interface (ODI) 157
Open Data-Link Interface, see ODI
OS/2 Remote Access Services Client
  CFMODEM 315
  Installation 313
  Modem 314
  Shuttle Feature 316
OS/2 Remote Workstation 313
OS/2 Warp Server Client Integrated Installation 313
OS/2 Warp Server Gateway 32

P

passphrase
  protecting 339
  rules 336
passphrases 332
PASSWD environment variable 187
PASSWD file 246
password key 332
password phrase 332
  protecting 339
  rules 336
PhoneBook 305
PING program 263
policy options, security 336
port connection managers 366, 369
  integrated PCMs 370
  stand-alone 369
PRELOADCACHE parameter, see TCPBEUI

PROTMAN.OS2 128
protocol manager, ANDI 372
Protocol Manager, see NDIS
PROTOCOL.INI 128, 130, 148, 149, 162, 264, 266, 267, 274
PSTN 303, 305

R

RAID
  Installation Considerations 13
READMAC.TXT file 126, 133
Remote Access Services 281
  Action List 290
  Adding Lines 324
  Answer Modes 303
  Application Considerations 356
  architecture 365
  Bridge Configuration 298
  Bridge Number 298
  Bridging 358
  Client System Requirements 286
  Concepts 281
  CONFIG.SYS 289
  Configuration 290
  Deinstallation 322
  Disk Space 285
  Enhancements 281
  Environments 283
    LAN-to-LAN 283
    LAN-to-Remote 283
    Remote-to-Central 283
    Remote-to-LAN 283
    Remote-to-Remote 283
  Filtering 298, 358
  Hops 298
  Inactivity Timeout Feature 323
  Installing 287
  Introduction 281
  LAN Distance 281
  LAN Requester 356
  LAN Segment Number 298
  LAN Server 356
  Maximum Addresses 301
  Maximum Data Unit Size 298
  Modem Classes 309
  Modem Configuration 295
  MPTS 311
  NetBIOS 311
  NetBIOS Timers 356
  NetWare 358
  Network Address 301
  OS/2 Client Installation 313
  Overview 281
  PhoneBook 305
  PIF files 363
  PROTOCOL.INI 289
  Security 331
  Security Database Tools 354
Remote Access Services *(continued)*
  Security Features 331
  Segment Numbers 358
  Setting up 286
  Settings Notebook 292
  Shared User Database 353
  Supported Clients 284
  System Requirements 285
  Uncertified Modems 363
  user types 332
  WAN Port 293
  Workstation 304
Remote Access Services Autostart Program 310
Remote Access Services Client Shuttle Feature 316
Remote Access Services Configurations 283
Remote Access Services Integrated Installation 287
Remote Access Services Naming 304
Remote Workstation 281
  relationship with connection server 373
RESOLV2 file 197
RFC encoded NetBIOS names, see TCPBEUI 267
RFCADDR.EXE program 266
RFCBCST.LST file 265
RFCCACHE.LST file 266
RFCNAMES.LST file 265
RHOSTS file 187, 197
Ring 3 33
ROUTE program 263
RSA encryption standard, see Cryptography

S

SAP 362
security
  administrator 332
  callback function 337
  Database Tools - Remote Access Services 354
  hash algorithm 332
  message authentication codes 333
  password key 332
  password phrase 339
  password phrases 332
    rules 336
  policy options 336
  session key 335
  user authentication protocol 333
  user types 332
  valid logon time intervals 339
  workstation address identification 339
Security - Remote 331
security administrator - Remote Access Services 332
Security Features 331
Segment Numbers 358
SENDMAIL.CF 196
SENDMAIL.UML file 197
server certificate 335
session key 335

SETUP.CMD file 196, 228, 274
Shared User Database - Remote Access Services 353
SIDEBAND parameter, see Adapter and Protocol Services
single logon 333
SNMP.INI file 197
Socket/MPTS
  configuration 144
  Converged Stack 132
  DHCP client 146
  MPTS 131
  native Sockets services 133
  native transport 132
  NetBIOS hostname 148
  NetBIOS Socket access 147
  non-native Sockets services 133
  non-native transport 132
  overview 132
  Socket/Multiprotocol Transport Services 131
  TCP/IP Socket access 144
Socket/Multiprotocol Transport Services, see Socket/MPTS
Sockets interface 131
Source address 362
SRVHEURISTICS - Remote Access Services 357
stand-alone PCMs 369
Switched Lines 305
Synchronous 309
SYSLOG.CNF file 226, 236

T

TCP/IP Services
  additional configuration 173
  basic functions 169
  Bootp 169, 197
  BootP message format 203
  BootP server 198
  Bootstrap Protocol 197
  common gateway interface (CGI) 250
  configuration files 196
  configure access security 184
  configure general parameters 183
  configure hostnames and nameservers 179
  configure internet servers 188
  configure network interfaces 174
  configure remote printing 189
  configure routers 178
  configure sendmail 191
  configure services to autostart 182
  configure SNMP 193
  configure Ultimail Lite 189
  corrective service diskettes (CSD) 247, 249, 255
  customer assistance program 243
  DHCP message format 202
  DHCP message types 202
  Domain Name System 216
  Domain Nameserver 265, 266
TCP/IP Services *(continued)*
  electronic mail 169, 189, 191
  expanding capabilities 246
  file transfer 169, 185, 244
  firewall 252
  fixed disk requirements 169
  FTP API 254
  Gopher 169, 244
  hosts file 266
  hypertext markup language (HTML) 250
  hypertext transfer protocol (HTTP) 250
  IBM Internet Connection family 250
  IBM Internet Connection for OS/2 242, 244
  IBM Internet Connection Server for OS/2 Warp 246, 250
  INETD super server daemon 183
  initial configuration 172
  installation 171
  Internet access 241
  Internet clients 169
  Internet dialer program 244
  Internet registration 242
  memory requirements 170
  Network File System 246
  Network File System kit 246
  new functions 168
  NewReader/2 244
  NewsReader/2 169
  NFS 246
  NFS access permissions 44
  NFS case sensitivity 45
  NFS client 43, 246, 247, 248
  NFS file locking 45
  NFS server 246
  NFS-mounted drive 43
  OSF Motif kit 255
  PCNFSD program 246
  Portmapper program 248
  PPP dial-up support 169
  Programmer's toolkit 254
  protocol stack 169
  proxy gateway 253
  publications 258
  remote execution 169, 187
  remote login 169, 185, 244
  remote printing 169, 189
  retrieve software updates over the Internet 246
  REXX FTP API 254
  REXX Sockets API 254
  Routing Information Protocol 169
  secure HTTP (S-HTTP) 250
  SLIP dial-up support 169
  SNA LU6.2 support 255
  SNMP DPI API 254
  Sockets API 254
  Socks API 253
  Socks server 253
  socksified application 253

TCP/IP Services *(continued)*
TCP/IP client and server functions 256
TCP/IP Internet access gateway 46
TCP/IP NFS file-sharing gateway 43
TCP/IP remote printing gateway 45
virtual device drivers 169, 255
WAN connectivity 255
WebExplorer 169, 244
WinSock 1.1 interface 255
X Window System 246
X Window System Client kit 254
X Window System Server (PMX) 249
X Window System Server kit 248
X.25 support 255
TCPBEUI
1000 client support 271
B-node 260
broadcast file 265
broadcast frames 264
coexistence 262
configure routing extensions 265
dial-up connections 273
directed broadcast 265
Domain Nameserver 265, 266
DOMAINSCOPE parameter 265, 266, 267, 270
dual protocol stack 275
H-node 241
hosts file 266
keepalive parameter 274
LM10 API 261, 262
M-node 241, 260
MAPNAME utility 267, 268
name cache 266
name discovery algorithm 266
NAMECACHE parameter 266
names file 264
NAMESFILE parameter 264
NetBIOS datagram distribution server 270
NetBIOS Domain Scope String 265
NetBIOS name server 270
NetBIOS over TCP/IP 260
NETBIOSRETRIES parameter 274
NETBIOSTIMEOUT parameter 274
P-node 241, 260
PACKETS parameter 275
performance 273
PRELOADCACHE parameter 266
removing 275
RFC 1001/1002 261, 270
RFC encoded NetBIOS names 267
routing extensions 264
structure diagram 261
TCPBEUI 260
TCPBEUI RAM usage 138
tuning 274
XMITBUFSIZE parameter 274
TCPOS2.INI file 196
TCPSTART.CMD 196
TELNET.PASSWORD.ID environment variable 185
TRUSERS file 185, 197
Tuning Assistance
capacity 15, 16
considerations 15
performance 15
remote access services 16
warnings/recommendations 16

U

Uncertified Modems 363
updateDNS string 231
USE_HOSTS_FIRST. environment variable 181
user - Remote Access Services 332
user accounts database 332
USER environment variable 184
user types 332

V

V.22 309
V.32 309
virtual LAN 366, 371

W

WAN Link 281
WAN Ports 324
WebExplorer, see TCP/IP Services
Windows Internet Name Service (WINS) 241
Windows Remote Access Services Client Installation 317
workstation address identification 339
WSTUNE.EXE parameters 18

X

X Window System, see TCP/IP Services

SG24-4602-00

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber

Inside OS/2 Warp Server, Volume 1: Exploring the Core Components

SG24-4602-00